

## » **google\_\_active\_\_folder**

Get an active folder within GCP by `display_name` and `parent`.

### » **Example Usage**

```
data "google_active_folder" "department1" {
  display_name = "Department 1"
  parent      = "organizations/1234567"
}
```

### » **Argument Reference**

The following arguments are supported:

- `display_name` - (Required) The folder's display name.
- `parent` - (Required) The resource name of the parent Folder or Organization.

### » **Attributes Reference**

In addition to the arguments listed above, the following attributes are exported:

- `name` - The resource name of the Folder. This uniquely identifies the folder.

## » **google\_\_billing\_\_account**

Use this data source to get information about a Google Billing Account.

```
data "google_billing_account" "acct" {
  display_name = "My Billing Account"
  open        = true
}
```

```
resource "google_project" "my_project" {
  name          = "My Project"
  project_id    = "your-project-id"
  org_id        = "1234567"

  billing_account = "${data.google_billing_account.acct.id}"
}
```

## » Argument Reference

The arguments of this data source act as filters for querying the available billing accounts. The given filters must match exactly one billing account whose data will be exported as attributes. The following arguments are supported:

- `billing_account` (Optional) - The name of the billing account in the form `{billing_account_id}` or `billingAccounts/{billing_account_id}`.
- `display_name` (Optional) - The display name of the billing account.
- `open` (Optional) - `true` if the billing account is open, `false` if the billing account is closed.

**NOTE:** One of `billing_account` or `display_name` must be specified.

## » Attributes Reference

The following additional attributes are exported:

- `id` - The billing account ID.
- `name` - The resource name of the billing account in the form `billingAccounts/{billing_account_id}`.
- `project_ids` - The IDs of any projects associated with the billing account.

## » `google_client_config`

Use this data source to access the configuration of the Google Cloud provider.

## » Example Usage

```
data "google_client_config" "current" {}

output "project" {
  value = "${data.google_client_config.current.project}"
}
```

## » Example Usage: Configure Kubernetes provider with OAuth2 access token

```
data "google_client_config" "default" {}

data "google_container_cluster" "my_cluster" {
  name     = "my-cluster"
  zone     = "us-east1-a"
```

```

}

provider "kubernetes" {
  load_config_file = false

  host = "https://${data.google_container_cluster.my_cluster.endpoint}"
  token = "${data.google_client_config.default.access_token}"
  cluster_ca_certificate = "${base64decode(data.google_container_cluster.my_cluster.master_certificate_data)}"
}

```

## » Argument Reference

There are no arguments available for this data source.

## » Attributes Reference

In addition to the arguments listed above, the following attributes are exported:

- `project` - The ID of the project to apply any resources to.
- `region` - The region to operate under.
- `access_token` - The OAuth2 access token used by the client to authenticate against the Google Cloud API.

## » `google_client_openid_userinfo`

Get OpenID userinfo about the credentials used with the Google provider, specifically the email.

When the `https://www.googleapis.com/auth/userinfo.email` scope is enabled in your provider block, this datasource enables you to export the email of the account you've authenticated the provider with; this can be used alongside `data.google_client_config`'s `access_token` to perform OpenID Connect authentication with GKE and configure an RBAC role for the email used.

This resource will only work as expected if the provider is configured to use the `https://www.googleapis.com/auth/userinfo.email` scope! You will receive an error otherwise.

## » Example Usage - exporting an email

```

provider "google" {
  scopes = [

```

```

    "https://www.googleapis.com/auth/compute",
    "https://www.googleapis.com/auth/cloud-platform",
    "https://www.googleapis.com/auth/ndev.clouddns.readwrite",
    "https://www.googleapis.com/auth/devstorage.full_control",
    "https://www.googleapis.com/auth/userinfo.email",
  ]
}

data "google_client_openid_userinfo" "me" {}

output "my-email" {
  value = "${data.google_client_openid_userinfo.me.email}"
}

```

## » Example Usage - OpenID Connect w/ Kubernetes provider + RBAC IAM role

```

provider "google" {
  scopes = [
    "https://www.googleapis.com/auth/compute",
    "https://www.googleapis.com/auth/cloud-platform",
    "https://www.googleapis.com/auth/ndev.clouddns.readwrite",
    "https://www.googleapis.com/auth/devstorage.full_control",
    "https://www.googleapis.com/auth/userinfo.email",
  ]
}

data "google_client_openid_userinfo" "provider_identity" {}

data "google_client_config" "provider" {}

data "google_container_cluster" "my_cluster" {
  name     = "my-cluster"
  zone     = "us-east1-a"
}

provider "kubernetes" {
  load_config_file = false

  host = "https://${data.google_container_cluster.my_cluster.endpoint}"
  token = "${data.google_client_config.provider.access_token}"
  cluster_ca_certificate = "${base64decode(data.google_container_cluster.my_cluster.master_a
}

resource "kubernetes_cluster_role_binding" "user" {

```

```

metadata {
  name = "provider-user-admin"
}

role_ref {
  api_group = "rbac.authorization.k8s.io"
  kind      = "ClusterRole"
  name      = "cluster-admin"
}

subject {
  kind = "User"
  name = "${data.google_client_openid_useremail.provider_identity.email}"
}
}

```

## » Argument Reference

There are no arguments available for this data source.

## » Attributes Reference

The following attributes are exported:

- **email** - The email of the account used by the provider to authenticate with GCP.

## » google\_cloudfunctions\_function

Get information about a Google Cloud Function. For more information see the official documentation and API.

## » Example Usage

```

data "google_cloudfunctions_function" "my-function" {
  name = "function"
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of a Cloud Function.

- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
  - **region** - (Optional) The region in which the resource belongs. If it is not provided, the provider region is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **name** - The name of the Cloud Function.
- **source\_archive\_bucket** - The GCS bucket containing the zip archive which contains the function.
- **source\_archive\_object** - The source archive object (file) in archive bucket.
- **description** - Description of the function.
- **available\_memory\_mb** - Available memory (in MB) to the function.
- **timeout** - Function execution timeout (in seconds).
- **runtime** - The runtime in which the function is running.
- **entry\_point** - Name of a JavaScript function that will be executed when the Google Cloud Function is triggered.
- **trigger\_http** - If function is triggered by HTTP, this boolean is set.
- **event\_trigger** - A source that fires events in response to a condition in another service. Structure is documented below.
- **https\_trigger\_url** - If function is triggered by HTTP, trigger URL is set here.
- **labels** - A map of labels applied to this function.

The **event\_trigger** block contains:

- **event\_type** - The type of event being observed. For example: `"providers/cloud.storage/eventTypes/object.change"` and `"providers/cloud.pubsub/eventTypes/topic.publish"`. See the documentation on calling Cloud Functions for a full reference.
- **resource** - The name of the resource whose events are being observed, for example, `"myBucket"`
- **failure\_policy** - Policy for failed executions. Structure is documented below.

The **failure\_policy** block supports:

- **retry** - Whether the function should be retried on failure.

## » google\_\_compute\_\_address

Get the IP address from a static address. For more information see the official API documentation.

### » Example Usage

```
data "google_compute_address" "my_address" {
  name = "foobar"
}

resource "google_dns_record_set" "frontend" {
  name = "frontend.${google_dns_managed_zone.prod.dns_name}"
  type = "A"
  ttl  = 300

  managed_zone = "${google_dns_managed_zone.prod.name}"

  rrrdatas = ["${data.google_compute_address.my_address.address}"]
}

resource "google_dns_managed_zone" "prod" {
  name      = "prod-zone"
  dns_name = "prod.mydomain.com."
}
```

### » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique name for the resource, required by GCE.
- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
  - **region** - (Optional) The Region in which the created address reside. If it is not provided, the provider region is used.

### » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **self\_link** - The URI of the created resource.
- **address** - The IP of the created resource.
- **status** - Indicates if the address is used. Possible values are: RESERVED or IN\_USE.

## » **google\_compute\_backend\_service**

Provide access to a Backend Service's attribute. For more information see the official documentation and the API.

### » **Example Usage**

```
data "google_compute_backend_service" "baz" {
  name = "foobar"
}
```

### » **Argument Reference**

The following arguments are supported:

- **name** - (Required) The name of the Backend Service.
- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.

### » **Attributes Reference**

In addition to the arguments listed above, the following attributes are exported:

- **connection\_draining\_timeout\_sec** - Time for which instance will be drained (not accept new connections, but still work to finish started ones).
- **description** - Textual description for the Backend Service.
- **enable\_cdn** - Whether or not Cloud CDN is enabled on the Backend Service.
- **fingerprint** - The fingerprint of the Backend Service.
- **port\_name** - The name of a service that has been added to an instance group in this backend.
- **protocol** - The protocol for incoming requests.



- **self\_link** - The URI of the Backend Service.
- **session\_affinity** - The Backend Service session stickyness configuration.
- **timeout\_sec** - The number of seconds to wait for a backend to respond to a request before considering the request failed.
- **backend** - The list of backends that serve this Backend Service.
- **health\_checks** - The list of HTTP/HTTPS health checks used by the Backend Service.

## » **google\_\_compute\_\_default\_\_service\_\_account**

Use this data source to retrieve default service account for this project

### » **Example Usage**

```
data "google_compute_default_service_account" "default" { }
```

```
output "default_account" {
  value = "${data.google_compute_default_service_account.default.email}"
}
```

### » **Argument Reference**

The following arguments are supported:

- **project** - (Optional) The project ID. If it is not provided, the provider project is used.

### » **Attributes Reference**

The following attributes are exported:

- **email** - Email address of the default service account used by VMs running in this project
- **unique\_id** - The unique id of the service account.
- **name** - The fully-qualified name of the service account.
- **display\_name** - The display name for the service account.

## » **google\_\_compute\_\_forwarding\_\_rule**

Get a forwarding rule within GCE from its name.

### » **Example Usage**

```
data "google_compute_forwarding_rule" "my-forwarding-rule" {  
  name = "forwarding-rule-us-east1"  
}
```

### » **Argument Reference**

The following arguments are supported:

- **name** - (Required) The name of the forwarding rule.
- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
  - **region** - (Optional) The region in which the resource belongs. If it is not provided, the project region is used.

### » **Attributes Reference**

In addition to the arguments listed above, the following attributes are exported:

- **description** - Description of this forwarding rule.
- **network** - Network of this forwarding rule.
- **subnetwork** - Subnetwork of this forwarding rule.
- **ip\_address** - IP address of this forwarding rule.
- **ip\_protocol** - IP protocol of this forwarding rule.
- **ports** - List of ports to use for internal load balancing, if this forwarding rule has any.
- **port\_range** - Port range, if this forwarding rule has one.
- **target** - URL of the target pool, if this forwarding rule has one.
- **backend\_service** - Backend service, if this forwarding rule has one.
- **load\_balancing\_scheme** - Type of load balancing of this forwarding rule.
- **region** - Region of this forwarding rule.

- `self_link` - The URI of the resource.

## » `google_compute_global_address`

Get the IP address from a static address reserved for a Global Forwarding Rule which are only used for HTTP load balancing. For more information see the official API documentation.

### » Example Usage

```
data "google_compute_global_address" "my_address" {
  name = "foobar"
}

resource "google_dns_record_set" "frontend" {
  name = "lb.${google_dns_managed_zone.prod.dns_name}"
  type = "A"
  ttl  = 300

  managed_zone = "${google_dns_managed_zone.prod.name}"

  rrdatas = ["${data.google_compute_global_address.my_address.address}"]
}

resource "google_dns_managed_zone" "prod" {
  name      = "prod-zone"
  dns_name = "prod.mydomain.com."
}
```

### » Argument Reference

The following arguments are supported:

- `name` - (Required) A unique name for the resource, required by GCE.
- 
- `project` - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **self\_link** - The URI of the created resource.
- **address** - The IP of the created resource.
- **status** - Indicates if the address is used. Possible values are: RESERVED or IN\_USE.

## » google\_compute\_image

Get information about a Google Compute Image. Check that your service account has the `compute.imageUser` role if you want to share custom images from another project. If you want to use public images, do not forget to specify the dedicated project. For more information see the official documentation and its API.

## » Example Usage

```
data "google_compute_image" "my_image" {
  name      = "debian-9"
  project   = "debian-cloud"
}

resource "google_compute_instance" "default" {
  # ...

  boot_disk {
    initialize_params {
      image = "${data.google_compute_image.my_image.self_link}"
    }
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** or **family** - (Required) The name of a specific image or a family. Exactly one of **name** or **family** must be specified. If **name** is specified, it will fetch the corresponding image. If **family** is specified, it will return the latest image that is part of an image family and is not deprecated.

- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used. If you are using a public base image, be sure to specify the correct Image Project.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **self\_link** - The URI of the image.
- **name** - The name of the image.
- **family** - The family name of the image.
- **disk\_size\_gb** - The size of the image when restored onto a persistent disk in gigabytes.
- **archive\_size\_bytes** - The size of the image tar.gz archive stored in Google Cloud Storage in bytes.
- **image\_id** - The unique identifier for the image.
- **image\_encryption\_key\_sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this image.
- **source\_image\_id** - The ID value of the image used to create this image.
- **source\_disk** - The URL of the source disk used to create this image.
- **source\_disk\_encryption\_key\_sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this image.
- **source\_disk\_id** - The ID value of the disk used to create this image.
- **creation\_timestamp** - The creation timestamp in RFC3339 text format.
- **description** - An optional description of this image.
- **labels** - A map of labels applied to this image.
- **label\_fingerprint** - A fingerprint for the labels being applied to this image.
- **licenses** - A list of applicable license URI.
- **status** - The status of the image. Possible values are **FAILED**, **PENDING**, or **READY**.

## » google\_\_compute\_\_instance

Get information about a VM instance resource within GCE. For more information see the official documentation and API.

## » Example Usage

```
data "google_compute_instance" "appserver" {
  name = "primary-application-server"
  zone = "us-central1-a"
}
```

## » Argument Reference

The following arguments are supported:

- **self\_link** - (Optional) The self link of the instance. One of **name** or **self\_link** must be provided.
  - **name** - (Optional) The name of the instance. One of **name** or **self\_link** must be provided.
- 
- **project** - (Optional) The ID of the project in which the resource belongs. If **self\_link** is provided, this value is ignored. If neither **self\_link** nor **project** are provided, the provider project is used.
  - **zone** - (Optional) The zone of the instance. If **self\_link** is provided, this value is ignored. If neither **self\_link** nor **zone** are provided, the provider zone is used.

## » Attributes Reference

- **boot\_disk** - The boot disk for the instance. Structure is documented below.
- **machine\_type** - The machine type to create.
- **network\_interface** - The networks attached to the instance. Structure is documented below.
- **attached\_disk** - List of disks attached to the instance. Structure is documented below.
- **can\_ip\_forward** - Whether sending and receiving of packets with non-matching source or destination IPs is allowed.
- **description** - A brief description of the resource.
- **deletion\_protection** - Whether deletion protection is enabled on this instance.
- **guest\_accelerator** - List of the type and count of accelerator cards attached to the instance. Structure is documented below.

- **labels** - A set of key/value label pairs assigned to the instance.
- **metadata** - Metadata key/value pairs made available within the instance.
- **min\_cpu\_platform** - The minimum CPU platform specified for the VM instance.
- **scheduling** - The scheduling strategy being used by the instance.
- **scratch\_disk** - The scratch disks attached to the instance. Structure is documented below.
- **service\_account** - The service account to attach to the instance. Structure is documented below.
- **tags** - The list of tags attached to the instance.
- **instance\_id** - The server-assigned unique identifier of this instance.
- **metadata\_fingerprint** - The unique fingerprint of the metadata.
- **self\_link** - The URI of the created resource.
- **tags\_fingerprint** - The unique fingerprint of the tags.
- **label\_fingerprint** - The unique fingerprint of the labels.
- **cpu\_platform** - The CPU platform used by this instance.
- **network\_interface.0.network\_ip** - The internal ip address of the instance, either manually or dynamically assigned.
- **network\_interface.0.access\_config.0.nat\_ip** - If the instance has an access config, either the given external ip (in the **nat\_ip** field) or the ephemeral (generated) ip (if you didn't provide one).
- **attached\_disk.0.disk\_encryption\_key\_sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.
- **boot\_disk.disk\_encryption\_key\_sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.
- **disk.0.disk\_encryption\_key\_sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.

---

The **boot\_disk** block supports:

- **auto\_delete** - Whether the disk will be auto-deleted when the instance is deleted.

- `device_name` - Name with which attached disk will be accessible under `/dev/disk/by-id/`
- `initialize_params` - Parameters with which a disk was created alongside the instance. Structure is documented below.
- `source` - The name or `self_link` of an existing disk (such as those managed by `google_compute_disk`) that was attached to the instance.

The `initialize_params` block supports:

- `size` - The size of the image in gigabytes.
- `type` - The GCE disk type. One of `pd-standard` or `pd-ssd`.
- `image` - The image from which this disk was initialised.

The `scratch_disk` block supports:

- `interface` - The disk interface used for attaching this disk. One of `SCSI` or `NVME`.

The `attached_disk` block supports:

- `source` - The name or `self_link` of the disk attached to this instance.
- `device_name` - Name with which the attached disk is accessible under `/dev/disk/by-id/`
- `mode` - Read/write mode for the disk. One of `"READ_ONLY"` or `"READ_WRITE"`.

The `network_interface` block supports:

- `network` - The name or `self_link` of the network attached to this interface.
- `subnetwork` - The name or `self_link` of the subnetwork attached to this interface.
- `subnetwork_project` - The project in which the subnetwork belongs.
- `network_ip` - The private IP address assigned to the instance.
- `access_config` - Access configurations, i.e. IPs via which this instance can be accessed via the Internet. Structure documented below.
- `alias_ip_range` - An array of alias IP ranges for this network interface. Structure documented below.

The `access_config` block supports:

- `nat_ip` - The IP address that is 1:1 mapped to the instance's network ip.
- `public_ptr_domain_name` - The DNS domain name for the public PTR record.



- `network_tier` - The networking tier used for configuring this instance. One of `PREMIUM` or `STANDARD`.

The `alias_ip_range` block supports:

- `ip_cidr_range` - The IP CIDR range represented by this alias IP range.
- `subnetwork_range_name` - The subnetwork secondary range name specifying the secondary range from which to allocate the IP CIDR range for this alias IP range.

The `service_account` block supports:

- `email` - The service account e-mail address.
- `scopes` - A list of service scopes.

The `scheduling` block supports:

- `preemptible` - Whether the instance is preemptible.
- `on_host_maintenance` - Describes maintenance behavior for the instance. One of `MIGRATE` or `TERMINATE`, for more info, read [here](#)
- `automatic_restart` - Specifies if the instance should be restarted if it was terminated by Compute Engine (not a user).

The `guest_accelerator` block supports:

- `type` - The accelerator type resource exposed to this instance. E.g. `nvidia-tesla-k80`.
- `count` - The number of the guest accelerator cards exposed to this instance.

## » `google_compute_instance_group`

Get a Compute Instance Group within GCE. For more information, see the [official documentation](#) and [API](#)

```
data "google_compute_instance_group" "all" {
  name = "instance-group-name"
  zone = "us-central1-a"
}
```

## » Argument Reference

The following arguments are supported:

- `name` - (Optional) The name of the instance group. Either `name` or `self_link` must be provided.

- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **self\_link** - (Optional) The self link of the instance group. Either **name** or **self\_link** must be provided.
- **zone** - (Optional) The zone of the instance group. If referencing the instance group by name and **zone** is not provided, the provider zone is used.

## » Attributes Reference

The following arguments are exported:

- **description** - Textual description of the instance group.
- **instances** - List of instances in the group.
- **named\_port** - List of named ports in the group.
- **network** - The URL of the network the instance group is in.
- **self\_link** - The URI of the resource.
- **size** - The number of instances in the group.

## » google\_compute\_lb\_ip\_ranges

Use this data source to access IP ranges in your firewall rules.

[https://cloud.google.com/compute/docs/load-balancing/health-checks#health\\_check\\_source\\_ips\\_and\\_firewall\\_rules](https://cloud.google.com/compute/docs/load-balancing/health-checks#health_check_source_ips_and_firewall_rules)

## » Example Usage

```
data "google_compute_lb_ip_ranges" "ranges" {}

resource "google_compute_firewall" "lb" {
  name      = "lb-firewall"
  network   = "${google_compute_network.main.name}"

  allow {
    protocol = "tcp"
    ports    = ["80"]
  }

  source_ranges = ["${data.google_compute_lb_ip_ranges.ranges.network}"]
}
```

```
target_tags = [
    "InstanceBehindLoadBalancer"
]
```

## » Argument Reference

There are no arguments available for this data source.

## » Attributes Reference

In addition to the arguments listed above, the following attributes are exported:

- **network** - The IP ranges used for health checks when **Network load balancing** is used
- **http\_ssl\_tcp\_internal** - The IP ranges used for health checks when **HTTP(S), SSL proxy, TCP proxy, and Internal load balancing** is used

## » google\_compute\_network

Get a network within GCE from its name.

## » Example Usage

```
data "google_compute_network" "my-network" {
  name = "default-us-east1"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the network.
- 
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following attributes are exported:

- **network** - The network name or resource link to the parent network of this network.
- **description** - Description of this network.
- **gateway\_ipv4** - The IP address of the gateway.
- **subnetworks\_self\_links** - the list of subnetworks which belong to the network
- **self\_link** - The URI of the resource.

## » google\_compute\_region\_instance\_group

Get a Compute Region Instance Group within GCE. For more information, see the official documentation and API.

```
data "google_compute_region_instance_group" "group" {
  name = "instance-group-name"
}
```

The most common use of this datasource will be to fetch information about the instances inside regional managed instance groups, for instance:

```
resource "google_compute_region_instance_group_manager" "foo" {
  name = "some_name"
  ...
  base_instance_name = "foo"
  ...
  instance_template = "${google_compute_instance_template.foo.self_link}"
  target_pools = ["${google_compute_target_pool.foo.self_link}"]
  ...
}

data "google_compute_region_instance_group" "data_source" {
  self_link = "${google_compute_region_instance_group_manager.foo.instance_group}"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Optional) The name of the instance group. One of **name** or **self\_link** must be provided.

- **self\_link** - (Optional) The link to the instance group. One of **name** or **self\_link** must be provided.

- 
- **project** - (Optional) The ID of the project in which the resource belongs. If **self\_link** is provided, this value is ignored. If neither **self\_link** nor **project** are provided, the provider project is used.
  - **region** - (Optional) The region in which the resource belongs. If **self\_link** is provided, this value is ignored. If neither **self\_link** nor **region** are provided, the provider region is used.

## » Attributes Reference

The following arguments are exported:

- **size** - The number of instances in the group.
- **instances** - List of instances in the group, as a list of resources, each containing:
  - **instance** - URL to the instance.
  - **named\_ports** - List of named ports in the group, as a list of resources, each containing:
    - \* **port** - Integer port number
    - \* **name** - String port name
  - **status** - String description of current state of the instance.

## » google\_\_project\_\_services

Use this data source to get details on the enabled project services.

For a list of services available, visit the API library page or run `gcloud services list`.

## » Example Usage

```
data "google_project_services" "project" {
  project = "your-project-id"
}

output "project_services" {
  value = "${join(",", data.google_project_services.project.services)}"
}
```

## » Argument Reference

The following arguments are supported:

- **project** - (Required) The project ID.

## » Attributes Reference

The following attributes are exported:

See `google_project_services` resource for details of the available attributes.

## » `google_compute_regions`

Provides access to available Google Compute regions for a given project. See more about regions and regions in the upstream docs.

```
data "google_compute_regions" "available" {}

resource "google_compute_subnetwork" "cluster" {
  count = "${length(data.google_compute_regions.available.names)}"
  name   = "my-network"
  ip_cidr_range = "10.36.${count.index}.0/24"
  network = "my-network"
  region  = "${data.google_compute_regions.available.names[count.index]}"
}
```

## » Argument Reference

The following arguments are supported:

- **project** (Optional) - Project from which to list available regions. Defaults to project declared in the provider.
- **status** (Optional) - Allows to filter list of regions based on their current status. Status can be either `UP` or `DOWN`. Defaults to no filtering (all available regions - both `UP` and `DOWN`).

## » Attributes Reference

The following attribute is exported:

- **names** - A list of regions available in the given project

## » **google\_\_compute\_\_ssl\_\_policy**

Gets an SSL Policy within GCE from its name, for use with Target HTTPS and Target SSL Proxies. For more information see the official documentation.

### » **Example Usage**

```
data "google_compute_ssl_policy" "my-ssl-policy" {  
  name = "production-ssl-policy"  
}
```

### » **Argument Reference**

The following arguments are supported:

- **name** - (Required) The name of the SSL Policy.
- 
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

### » **Attributes Reference**

In addition to the arguments listed above, the following attributes are exported:

- **enabled\_features** - The set of enabled encryption ciphers as a result of the policy config
- **description** - Description of this SSL Policy.
- **min\_tls\_version** - The minimum supported TLS version of this policy.
- **profile** - The Google-curated or custom profile used by this policy.
- **custom\_features** - If the **profile** is **CUSTOM**, these are the custom encryption ciphers supported by the profile. If the **profile** is *not* **CUSTOM**, this attribute will be empty.
- **fingerprint** - Fingerprint of this resource.
- **self\_link** - The URI of the created resource.

## » **google\_\_compute\_\_subnetwork**

Get a subnetwork within GCE from its name and region.

## » Example Usage

```
data "google_compute_subnetwork" "my-subnetwork" {
  name     = "default-us-east1"
  region   = "us-east1"
}
```

## » Argument Reference

The following arguments are supported:

- **self\_link** - (Optional) The self link of the subnetwork. If **self\_link** is specified, **name**, **project**, and **region** are ignored.
- **name** - (Optional) The name of the subnetwork. One of **name** or **self\_link** must be specified.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **region** - (Optional) The region this subnetwork has been created in. If unspecified, this defaults to the region configured in the provider.

## » Attributes Reference

In addition to the arguments listed above, the following attributes are exported:

- **network** - The network name or resource link to the parent network of this subnetwork.
- **description** - Description of this subnetwork.
- **ip\_cidr\_range** - The IP address range that machines in this network are assigned to, represented as a CIDR block.
- **gateway\_address** - The IP address of the gateway.
- **private\_ip\_google\_access** - Whether the VMs in this subnet can access Google services without assigned external IP addresses.
- **secondary\_ip\_range** - An array of configurations for secondary IP ranges for VM instances contained in this subnetwork. Structure is documented below.

The **secondary\_ip\_range** block supports:

- **range\_name** - The name associated with this subnetwork secondary range, used when adding an alias IP range to a VM instance.



- `ip_cidr_range` - The range of IP addresses belonging to this subnetwork secondary range.

## » `google__compute__vpn__gateway`

Get a VPN gateway within GCE from its name.

### » Example Usage

```
data "google_compute_vpn_gateway" "my-vpn-gateway" {
  name = "vpn-gateway-us-east1"
}
```

### » Argument Reference

The following arguments are supported:

- `name` - (Required) The name of the VPN gateway.
- 
- `project` - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
  - `region` - (Optional) The region in which the resource belongs. If it is not provided, the project region is used.

### » Attributes Reference

In addition to the arguments listed above, the following attributes are exported:

- `network` - The network of this VPN gateway.
- `description` - Description of this VPN gateway.
- `region` - Region of this VPN gateway.
- `self_link` - The URI of the resource.

## » `google__compute__zones`

Provides access to available Google Compute zones in a region for a given project. See more about regions and zones in the upstream docs.

```

data "google_compute_zones" "available" {}

resource "google_compute_instance_group_manager" "foo" {
  count = "${length(data.google_compute_zones.available.names)}"

  name           = "terraform-test-${count.index}"
  instance_template = "${google_compute_instance_template.foobar.self_link}"
  base_instance_name = "foobar-${count.index}"
  zone           = "${data.google_compute_zones.available.names[count.index]}"
  target_size     = 1
}

```

## » Argument Reference

The following arguments are supported:

- **project** (Optional) - Project from which to list available zones. Defaults to project declared in the provider.
- **region** (Optional) - Region from which to list available zones. Defaults to region declared in the provider.
- **status** (Optional) - Allows to filter list of zones based on their current status. Status can be either UP or DOWN. Defaults to no filtering (all available zones - both UP and DOWN).

## » Attributes Reference

The following attribute is exported:

- **names** - A list of zones available in the given region

## » google\_\_container\_\_cluster

Get info about a cluster within GKE from its name and zone.

## » Example Usage

```

data "google_container_cluster" "my_cluster" {
  name = "my-cluster"
  zone = "us-east1-a"
}

```

```

output "cluster_username" {

```

```

    value = "${data.google_container_cluster.my_cluster.master_auth.0.username}"
  }

  output "cluster_password" {
    value = "${data.google_container_cluster.my_cluster.master_auth.0.password}"
  }

  output "endpoint" {
    value = "${data.google_container_cluster.my_cluster.endpoint}"
  }

  output "instance_group_urls" {
    value = "${data.google_container_cluster.my_cluster.instance_group_urls}"
  }

  output "node_config" {
    value = "${data.google_container_cluster.my_cluster.node_config}"
  }

  output "node_pools" {
    value = "${data.google_container_cluster.my_cluster.node_pool}"
  }

```

## » Argument Reference

The following arguments are supported:

- **name** - The name of the cluster.
  - **zone** or **region** - The zone or region this cluster has been created in.
- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

See `google_container_cluster` resource for details of the available attributes.

## » `google__container__engine__versions`

Provides access to available Google Container Engine versions in a zone or region for a given project.

If you are using the `google_container_engine_versions` datasource with a regional cluster, ensure that you have provided a `region` to the datasource. A `region` can have a different set of supported versions than its corresponding zones, and not all zones in a `region` are guaranteed to support the same version.

## » Example Usage

```
data "google_container_engine_versions" "central1b" {
  zone           = "us-central1-b"
  version_prefix = "1.12."
}

resource "google_container_cluster" "foo" {
  name          = "terraform-test-cluster"
  zone          = "us-central1-b"
  node_version   = "${data.google_container_engine_versions.central1b.latest_node_version}"
  initial_node_count = 1

  master_auth {
    username = "mr.yoda"
    password = "adoy.rm"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **zone** (optional) - Zone to list available cluster versions for. Should match the zone the cluster will be deployed in. If not specified, the provider-level zone is used. One of zone or provider-level zone is required.
- **region** (optional, Beta) - Region to list available cluster versions for. Should match the region the cluster will be deployed in. For regional clusters, this value must be specified and cannot be inferred from provider-level region. One of zone, region, or provider-level zone is required.
- **project** (optional) - ID of the project to list available cluster versions for. Should match the project the cluster will be deployed to. Defaults to the project that the provider is authenticated with.
- **version\_prefix** (optional) - If provided, Terraform will only return versions that match the string prefix. For example, `1.11.` will match all `1.11` series releases. Since this is just a string match, it's recommended that you append a `.` after minor versions to ensure that prefixes such as

1.1 don't match versions like 1.12.5-gke.10 accidentally. See the docs on versioning schema for full details on how version strings are formatted.

## » Attributes Reference

The following attributes are exported:

- **valid\_master\_versions** - A list of versions available in the given zone for use with master instances.
- **valid\_node\_versions** - A list of versions available in the given zone for use with node instances.
- **latest\_master\_version** - The latest version available in the given zone for use with master instances.
- **latest\_node\_version** - The latest version available in the given zone for use with node instances.
- **default\_cluster\_version** - Version of Kubernetes the service deploys by default.

## » google\_container\_registry\_image

This data source fetches the project name, and provides the appropriate URLs to use for container registry for this project.

The URLs are computed entirely offline - as long as the project exists, they will be valid, but this data source does not contact Google Container Registry (GCR) at any point.

## » Example Usage

```
data "google_container_registry_image" "debian" {
  name = "debian"
}

output "gcr_location" {
  value = "${data.google_container_registry_image.debian.image_url}"
}
```

## » Argument Reference

- **name:** (Required) The image name.
- **project:** (Optional) The project ID that this image is attached to. If not provider, provider project will be used instead.

- **region:** (Optional) The GCR region to use. As of this writing, one of **asia**, **eu**, and **us**. See the documentation for additional information.
- **tag:** (Optional) The tag to fetch, if any.
- **digest:** (Optional) The image digest to fetch, if any.

## » Attributes Reference

In addition to the arguments listed above, this data source exports: \* **image\_url:** The URL at which the image can be accessed.

## » google\_container\_registry\_repository

This data source fetches the project name, and provides the appropriate URLs to use for container registry for this project.

The URLs are computed entirely offline - as long as the project exists, they will be valid, but this data source does not contact Google Container Registry (GCR) at any point.

## » Example Usage

```
data "google_container_registry_repository" "foo" {}

output "gcr_location" {
  value = "${data.google_container_registry_repository.foo.repository_url}"
}
```

## » Argument Reference

- **project:** (Optional) The project ID that this repository is attached to. If not provided, provider project will be used instead.
- **region:** (Optional) The GCR region to use. As of this writing, one of **asia**, **eu**, and **us**. See the documentation for additional information.

## » Attributes Reference

In addition to the arguments listed above, this data source exports:

- **repository\_url:** The URL at which the repository can be accessed.

## » google\_\_dns\_\_managed\_\_zone

Provides access to a zone's attributes within Google Cloud DNS. For more information see the official documentation and API.

```
data "google_dns_managed_zone" "env_dns_zone" {
  name      = "qa-zone"
}

resource "google_dns_record_set" "dns" {
  name = "my-address.${data.google_dns_managed_zone.env_dns_zone.dns_name}"
  type = "TXT"
  ttl  = 300

  managed_zone = "${data.google_dns_managed_zone.env_dns_zone.name}"

  rrdatas = ["test"]
}
```

## » Argument Reference

- **name** - (Required) A unique name for the resource.
- **project** - (Optional) The ID of the project for the Google Cloud DNS zone.

## » Attributes Reference

The following attributes are exported:

- **dns\_name** - The fully qualified DNS name of this zone, e.g. **terraform.io**.
- **description** - A textual description field.
- **name\_servers** - The list of nameservers that will be authoritative for this domain. Use NS records to redirect from your DNS provider to these names, thus making Google Cloud DNS authoritative for this zone.

## » google\_\_folder

Use this data source to get information about a Google Cloud Folder.

```
# Get folder by id
data "google_folder" "my_folder_1" {
  folder = "folders/12345"
}
```

```

    lookup_organization = true
  }

# Search by fields
data "google_folder" "my_folder_2" {
  folder = "folders/23456"
}

output "my_folder_1_organization" {
  value = "${data.google_folder.my_folder_1.organization}"
}

output "my_folder_2_parent" {
  value = "${data.google_folder.my_folder_2.parent}"
}

```

## » Argument Reference

The following arguments are supported:

- **folder** (Required) - The name of the Folder in the form `{folder_id}` or `folders/{folder_id}`.
- **lookup\_organization** (Optional) - `true` to find the organization that the folder belongs, `false` to avoid the lookup. It searches up the tree. (defaults to `false`)

## » Attributes Reference

The following attributes are exported:

- **id** - The Folder ID.
- **name** - The resource name of the Folder in the form `folders/{folder_id}`.
- **parent** - The resource name of the parent Folder or Organization.
- **display\_name** - The folder's display name.
- **create\_time** - Timestamp when the Organization was created. A timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds. Example: "2014-10-02T15:01:23.045123456Z".
- **lifecycle\_state** - The Folder's current lifecycle state.
- **organization** - If `lookup_organization` is enable, the resource name of the Organization that the folder belongs.



## » google\_iam\_policy

Generates an IAM policy document that may be referenced by and applied to other Google Cloud Platform resources, such as the `google_project` resource.

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/compute.instanceAdmin"

    members = [
      "serviceAccount:your-custom-sa@your-project.iam.gserviceaccount.com",
    ]
  }

  binding {
    role = "roles/storage.objectViewer"

    members = [
      "user:alice@gmail.com",
    ]
  }

  audit_config {
    service = "cloudkms.googleapis.com"
    audit_log_configs {
      log_type = "DATA_READ",
      exempted_members = ["user:you@domain.com"]
    }

    audit_log_configs {
      log_type = "DATA_WRITE",
    }

    audit_log_configs {
      log_type = "ADMIN_READ",
    }
  }
}
```

This data source is used to define IAM policies to apply to other resources. Currently, defining a policy through a datasource and referencing that policy from another resource is the only way to apply an IAM policy to a resource.

**Note:** Several restrictions apply when setting IAM policies through this API. See the `setIamPolicy` docs for a list of these restrictions.

## » Argument Reference

The following arguments are supported:

- **binding** (Required) - A nested configuration block (described below) defining a binding to be included in the policy document. Multiple **binding** arguments are supported.

Each document configuration must have one or more **binding** blocks, which each accept the following arguments:

- **role** (Required) - The role/permission that will be granted to the members. See the IAM Roles documentation for a complete list of roles. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **members** (Required) - An array of identities that will be granted the privilege in the **role**. For more details on format and restrictions see <https://cloud.google.com/billing/reference/rest/v1/Policy#Binding> Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account. It **can't** be used with the `google_project` resource.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account. It **can't** be used with the `google_project` resource.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **audit\_config** (Optional) - A nested configuration block that defines logging additional configuration for your project.
  - **service** (Required) Defines a service that will be enabled for audit logging. For example, `storage.googleapis.com`, `cloudsql.googleapis.com`. `allServices` is a special value that covers all services.
  - **audit\_log\_configs** (Required) A nested block that defines the operations you'd like to log.
  - **log\_type** (Required) Defines the logging level. `DATA_READ`, `DATA_WRITE` and `ADMIN_READ` capture different types of events. See

- the audit configuration documentation for more details.
- **exempted\_members** (Optional) Specifies the identities that are exempt from these types of logging operations. Follows the same format of the **members** array for **binding**.

## » Attributes Reference

The following attribute is exported:

- **policy\_data** - The above bindings serialized in a format suitable for referencing from a resource that supports IAM.

## » google\_iam\_role

Use this data source to get information about a Google IAM Role.

```
data "google_iam_role" "roleinfo" {
  name = "roles/compute.viewer"
}

output "the_role_permissions" {
  value = "${data.google_iam_role.roleinfo.included_permissions}"
}
```

## » Argument Reference

The following arguments are supported:

- **name** (Required) - The name of the Role to lookup in the form `roles/{ROLE_NAME}`, `organizations/{ORGANIZATION_ID}/roles/{ROLE_NAME}` or `projects/{PROJECT_ID}/roles/{ROLE_NAME}`

## » Attributes Reference

The following attributes are exported:

- **title** - is a friendly title for the role, such as "Role Viewer"
- **included\_permissions** - specifies the list of one or more permissions to include in the custom role, such as - `iam.roles.get`
- **stage** - indicates the stage of a role in the launch lifecycle, such as GA, BETA or ALPHA.

## » `google__kms__key__ring`

Provides access to Google Cloud Platform KMS KeyRing. For more information see the official documentation and API.

A KeyRing is a grouping of CryptoKeys for organizational purposes. A KeyRing belongs to a Google Cloud Platform Project and resides in a specific location.

### » Example Usage

```
data "google_kms_key_ring" "my_key_ring" {
  name      = "my-key-ring"
  location  = "us-central1"
}
```

### » Argument Reference

The following arguments are supported:

- `name` - (Required) The KeyRing's name. A KeyRing name must exist within the provided location and match the regular expression `[a-zA-Z0-9_-]{1,63}`
  - `location` - (Required) The Google Cloud Platform location for the KeyRing. A full list of valid locations can be found by running `gcloud kms locations list`.
- 
- `project` - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.

### » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `self_link` - The self link of the created KeyRing. Its format is `projects/{projectId}/locations/{location}/keyRings/{keyRingName}`.

## » `google__kms__crypto__key`

Provides access to a Google Cloud Platform KMS CryptoKey. For more information see the official documentation and API.

A `CryptoKey` is an interface to key material which can be used to encrypt and decrypt data. A `CryptoKey` belongs to a Google Cloud KMS KeyRing.

## » Example Usage

```
data "google_kms_key_ring" "my_key_ring" {
  name      = "my-key-ring"
  location  = "us-central1"
}

data "google_kms_crypto_key" "my_crypto_key" {
  name      = "my-crypto-key"
  key_ring  = "${data.google_kms_key_ring.my_key_ring.self_link}"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The `CryptoKey`'s name. A `CryptoKey`'s name belonging to the specified Google Cloud Platform KeyRing and match the regular expression `[a-zA-Z0-9_-]{1,63}`
- **key\_ring** - (Required) The **self\_link** of the Google Cloud Platform KeyRing to which the key belongs.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **rotation\_period** - Every time this period passes, generate a new `CryptoKeyVersion` and set it as the primary. The first rotation will take place after the specified period. The rotation period has the format of a decimal number with up to 9 fractional digits, followed by the letter s (seconds).
- **self\_link** - The self link of the created `CryptoKey`. Its format is `projects/{projectId}/locations/{location}/keyRings/{keyRingName}/cryptoKeys/{cryptoKeyName}`

## » google\_\_kms\_\_secret

This data source allows you to use data encrypted with Google Cloud KMS within your resource definitions.

For more information see the official documentation.

**NOTE:** Using this data provider will allow you to conceal secret data within your resource definitions, but it does not take care of protecting that data in the logging output, plan output, or state output. Please take care to secure your secret data outside of resource definitions.

## » Example Usage

First, create a KMS KeyRing and CryptoKey using the resource definitions:

```
resource "google_kms_key_ring" "my_key_ring" {
  project = "my-project"
  name    = "my-key-ring"
  location = "us-central1"
}

resource "google_kms_crypto_key" "my_crypto_key" {
  name      = "my-crypto-key"
  key_ring = "${google_kms_key_ring.my_key_ring.id}"
}
```

Next, use the Cloud SDK to encrypt some sensitive information:

```
$ echo -n my-secret-password | gcloud kms encrypt \
> --project my-project \
> --location us-central1 \
> --keyring my-key-ring \
> --key my-crypto-key \
> --plaintext-file - \
> --ciphertext-file - \
> | base64
CiQAQD+xX4SX0SziF4a8JYvq4spfAuWhhYSNu133H85HnVtNQW4S0gDu2UZ46dQCRF15MF6ekabviN8xq+F+2035ZJ8
```

Finally, reference the encrypted ciphertext in your resource definitions:

```
data "google_kms_secret" "sql_user_password" {
  crypto_key = "${google_kms_crypto_key.my_crypto_key.id}"
  ciphertext = "CiQAQD+xX4SX0SziF4a8JYvq4spfAuWhhYSNu133H85HnVtNQW4S0gDu2UZ46dQCRF15MF6ekabv"
}

resource "google_sql_database_instance" "master" {
  name = "master-instance"

  settings {
    tier = "DO"
  }
}
```

```
resource "google_sql_user" "users" {
  name      = "me"
  instance = "${google_sql_database_instance.master.name}"
  host      = "me.com"
  password = "${data.google_kms_secret.sql_user_password.plaintext}"
}
```

This will result in a Cloud SQL user being created with password my-secret-password.

## » Argument Reference

The following arguments are supported:

- **ciphertext** (Required) - The ciphertext to be decrypted, encoded in base64
- **crypto\_key** (Required) - The id of the CryptoKey that will be used to decrypt the provided ciphertext. This is represented by the format {projectId}/{location}/{keyRingName}/{cryptoKeyName}.

## » Attributes Reference

The following attribute is exported:

- **plaintext** - Contains the result of decrypting the provided ciphertext.

## » google\_\_netblock\_\_ip\_\_ranges

Use this data source to get the IP ranges from the sender policy framework (SPF) record of \_cloud-netblocks.googleusercontent

[https://cloud.google.com/compute/docs/faq#where\\_can\\_i\\_find\\_product\\_name\\_short\\_ip\\_ranges](https://cloud.google.com/compute/docs/faq#where_can_i_find_product_name_short_ip_ranges)

## » Example Usage

```
data "google_netblock_ip_ranges" "netblock" {}

output "cidr_blocks" {
  value = "${data.google_netblock_ip_ranges.netblock.cidr_blocks}"
}
```

```

output "cidr_blocks_ipv4" {
  value = "${data.google_netblock_ip_ranges.netblock.cidr_blocks_ipv4}"
}

output "cidr_blocks_ipv6" {
  value = "${data.google_netblock_ip_ranges.netblock.cidr_blocks_ipv6}"
}

```

## » Attributes Reference

- `cidr_blocks` - Retrieve list of all CIDR blocks.
- `cidr_blocks_ipv4` - Retrieve list of the IP4 CIDR blocks
- `cidr_blocks_ipv6` - Retrieve list of the IP6 CIDR blocks.

## » google\_\_organization

Use this data source to get information about a Google Cloud Organization.

```

data "google_organization" "org" {
  domain = "example.com"
}

resource "google_folder" "sales" {
  display_name = "Sales"
  parent       = "${data.google_organization.org.name}"
}

```

## » Argument Reference

The arguments of this data source act as filters for querying the available Organizations. The given filters must match exactly one Organizations whose data will be exported as attributes. The following arguments are supported:

- `organization` (Optional) - The name of the Organization in the form `{organization_id}` or `organizations/{organization_id}`.
- `domain` (Optional) - The domain name of the Organization.

**NOTE:** One of `organization` or `domain` must be specified.

## » Attributes Reference

The following additional attributes are exported:



- **id** - The Organization ID.
- **name** - The resource name of the Organization in the form **organizations/{organization\_id}**.
- **directory\_customer\_id** - The Google for Work customer ID of the Organization.
- **create\_time** - Timestamp when the Organization was created. A timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds. Example: "2014-10-02T15:01:23.045123456Z".
- **lifecycle\_state** - The Organization's current lifecycle state.

## » **google\_\_project**

Use this data source to get project details. For more information see API

### » **Example Usage**

```
data "google_project" "project" {}

output "project_number" {
  value = "${data.google_project.project.number}"
}
```

### » **Argument Reference**

The following arguments are supported:

- **project\_id** - (Optional) The project ID. If it is not provided, the provider project is used.

### » **Attributes Reference**

The following attributes are exported:

See `google__project` resource for details of the available attributes.

## » **google\_\_projects**

Retrieve information about a set of projects based on a filter. See the REST API for more details.

### » Example Usage - searching for projects about to be deleted in an org

```
data "google_projects" "my-org-projects" {
  filter = "parent.id:012345678910 lifecycleState:DELETE_REQUESTED"
}

data "google_project" "deletion-candidate" {
  project_id = "${data.google_projects.my-org-projects.projects.0.project_id}"
}
```

### » Argument Reference

The following arguments are supported:

- **filter** - (Optional) A string filter as defined in the REST API.

### » Attributes Reference

The following attributes are exported:

- **projects** - A list of projects matching the provided filter. Structure is defined below.

The **projects** block supports:

- **project\_id** - The project id of the project.

## » google\_service\_account

Get the service account from a project. For more information see the official API documentation.

### » Example Usage

```
data "google_service_account" "object_viewer" {
  account_id = "object-viewer"
}
```

## » Example Usage, save key in Kubernetes secret

```
data "google_service_account" "myaccount" {
  account_id = "myaccount-id"
}

resource "google_service_account_key" "mykey" {
  service_account_id = "${data.google_service_account.myaccount.name}"
}

resource "kubernetes_secret" "google-application-credentials" {
  metadata = {
    name = "google-application-credentials"
  }
  data {
    credentials.json = "${base64decode(google_service_account_key.mykey.private_key)}"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **account\_id** - (Required) The Service account id. (This is the part of the service account's email field that comes before the @ symbol.)
- **project** - (Optional) The ID of the project that the service account will be created in. Defaults to the provider project configuration.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **email** - The e-mail address of the service account. This value should be referenced from any `google_iam_policy` data sources that would grant the service account privileges.
- **unique\_id** - The unique id of the service account.
- **name** - The fully-qualified name of the service account.
- **display\_name** - The display name for the service account.

## » `google__service__account__key`

Get service account public key. For more information, see the official documentation and API.

### » Example Usage

```
resource "google_service_account" "myaccount" {
  account_id = "dev-foo-account"
}

resource "google_service_account_key" "mykey" {
  service_account_id = "${google_service_account.myaccount.name}"
}

data "google_service_account_key" "mykey" {
  name = "${google_service_account_key.mykey.name}"
  public_key_type = "TYPE_X509_PEM_FILE"
}
```

### » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the service account key. This must have format `projects/{PROJECT_ID}/serviceAccounts/{ACCOUNT}/keys/{KEYID}`, where `{ACCOUNT}` is the email address or unique id of the service account.
- **project** - (Optional) The ID of the project that the service account will be created in. Defaults to the provider project configuration.
- **public\_key\_type** (Optional) The output format of the public key requested. `X509_PEM` is the default output format.

### » Attributes Reference

The following attributes are exported in addition to the arguments listed above:

- **public\_key** - The public key, base64 encoded

## » google\_\_storage\_\_object\_\_signed\_\_url

The Google Cloud storage signed URL data source generates a signed URL for a given storage object. Signed URLs provide a way to give time-limited read or write access to anyone in possession of the URL, regardless of whether they have a Google account.

For more info about signed URL's is available [here](#).

### » Example Usage

```
data "google_storage_object_signed_url" "artifact" {
  bucket = "install_binaries"
  path   = "path/to/install_file.bin"
}

resource "google_compute_instance" "vm" {
  name = "vm"
  ...

  provisioner "remote-exec" {
    inline = [
      "wget '${data.google_storage_object_signed_url.artifact.signed_url}' -O install_file.bin",
      "chmod +x install_file.bin",
      "./install_file.bin"
    ]
  }
}
```

### » Full Example

```
data "google_storage_object_signed_url" "get_url" {
  bucket      = "fried_chicken"
  path        = "path/to/file"
  content_md5 = "pRviqwS4c40TJRTe03FD1w=="
  content_type = "text/plain"
  duration    = "2d"
  credentials = "${file("path/to/credentials.json")}"

  extension_headers = {
    x-goog-if-generation-match = 1
  }
}
```

## » Argument Reference

The following arguments are supported:

- **bucket** - (Required) The name of the bucket to read the object from
- **path** - (Required) The full path to the object inside the bucket
- **http\_method** - (Optional) What HTTP Method will the signed URL allow (defaults to **GET**)
- **duration** - (Optional) For how long shall the signed URL be valid (defaults to 1 hour - i.e. **1h**). See here for info on valid duration formats.
- **credentials** - (Optional) What Google service account credentials json should be used to sign the URL. This data source checks the following locations for credentials, in order of preference: data source **credentials** attribute, provider **credentials** attribute and finally the **GOOGLE\_APPLICATION\_CREDENTIALS** environment variable.

**NOTE** the default google credentials configured by **gcloud** sdk or the service account associated with a compute instance cannot be used, because these do not include the private key required to sign the URL. A valid **json** service account credentials key file must be used, as generated via Google cloud console.

- **content\_type** - (Optional) If you specify this in the datasource, the client must provide the **Content-Type** HTTP header with the same value in its request.
- **content\_md5** - (Optional) The MD5 digest value in Base64. Typically retrieved from **google\_storage\_bucket\_object.object.md5hash** attribute. If you provide this in the datasource, the client (e.g. browser, curl) must provide the **Content-MD5** HTTP header with this same value in its request.
- **extension\_headers** - (Optional) As needed. The server checks to make sure that the client provides matching values in requests using the signed URL. Any header starting with **x-goog-** is accepted but see the Google Docs for list of headers that are supported by Google.

## » Attributes Reference

The following attributes are exported:

- **signed\_url** - The signed URL that can be used to access the storage object without authentication.

## » `google__storage__bucket__object`

Gets an existing object inside an existing bucket in Google Cloud Storage service (GCS). See the official documentation and API.

### » Example Usage

Example picture stored within a folder.

```
data "google_storage_bucket_object" "picture" {
  name     = "folder/butterfly01.jpg"
  bucket   = "image-store"
}
```

### » Argument Reference

The following arguments are supported:

- `bucket` - (Required) The name of the containing bucket.
- `name` - (Required) The name of the object.

### » Attributes Reference

The following attributes are exported:

- `cache_control` - (Computed) Cache-Control directive to specify caching behavior of object data. If omitted and object is accessible to all anonymous users, the default will be public, max-age=3600
- `content_disposition` - (Computed) Content-Disposition of the object data.
- `content_encoding` - (Computed) Content-Encoding of the object data.
- `content_language` - (Computed) Content-Language of the object data.
- `content_type` - (Computed) Content-Type of the object data. Defaults to "application/octet-stream" or "text/plain; charset=utf-8".
- `crc32c` - (Computed) Base 64 CRC32 hash of the uploaded data.
- `md5hash` - (Computed) Base 64 MD5 hash of the uploaded data.
- `self_link` - (Computed) A url reference to this object.
- `storage_class` - (Computed) The StorageClass of the new bucket object. Supported values include: `MULTI_REGIONAL`, `REGIONAL`, `NEARLINE`,

COLDLINE. If not provided, this defaults to the bucket's default storage class or to a standard class.

## » `google_storage_project_service_account`

Get the email address of a project's unique Google Cloud Storage service account.

Each Google Cloud project has a unique service account for use with Google Cloud Storage. Only this special service account can be used to set up `google_storage_notification` resources.

For more information see the API reference.

## » Example Usage

```
data "google_storage_project_service_account" "gcs_account" {}

resource "google_pubsub_topic_iam_binding" "binding" {
  topic      = "${google_pubsub_topic.topic.name}"
  role       = "roles/pubsub.publisher"

  members    = ["serviceAccount:${data.google_storage_project_service_account.gcs_account}"]
}
```

## » Argument Reference

The following arguments are supported:

- `project` - (Optional) The project the unique service account was created for. If it is not provided, the provider project is used.
- `user_project` - (Optional) The project the lookup originates from. This field is used if you are making the request from a different account than the one you are finding the service account for.

## » Attributes Reference

The following attributes are exported:

- `email_address` - The email address of the service account. This value is often used to refer to the service account in order to grant IAM permissions.



## » google\_\_storage\_\_transfer\_\_project\_\_service\_\_account

Use this data source to retrieve Storage Transfer service account for this project

### » Example Usage

```
data "google_storage_transfer_project_service_account" "default" { }
```

```
output "default_account" {  
  value = "${data.google_storage_transfer_project_service_account.default.email}"  
}
```

### » Argument Reference

The following arguments are supported:

- **project** - (Optional) The project ID. If it is not provided, the provider project is used.

### » Attributes Reference

The following attributes are exported:

- **email** - Email address of the default service account used by Storage Transfer Jobs running in this project

## » google\_\_access\_\_context\_\_manager\_\_access\_\_level

An AccessLevel is a label that can be applied to requests to GCP services, along with a list of requirements necessary for the label to be applied.

**Warning:** This resource is in beta, and should be used with the terraform-provider-google-beta provider. See Provider Versions for more details on beta resources.

To get more information about AccessLevel, see:

- API documentation
- How-to Guides
  - Access Policy Quickstart

## » Example Usage - Access Context Manager Access Level Basic

```
resource "google_access_context_manager_access_level" "access-level" {
  parent      = "accessPolicies/${google_access_context_manager_access_policy.test-access.name}"
  name        = "accessPolicies/${google_access_context_manager_access_policy.test-access.name}/accessLevels/{short_name}"
  title       = "ios_no_lock"
  basic {
    conditions {
      device_policy {
        require_screen_lock = false
        os_constraints {
          os_type = "IOS"
        }
      }
    }
  }
}
```

```
resource "google_access_context_manager_access_policy" "access-policy" {
  parent = "organizations/123456789"
  title  = "my policy"
}
```

## » Argument Reference

The following arguments are supported:

- **title** - (Required) Human readable title. Must be unique within the Policy.
  - **parent** - (Required) The AccessPolicy this AccessLevel lives in. Format: accessPolicies/{policy\_id}
  - **name** - (Required) Resource name for the Access Level. The short\_name component must begin with a letter and only include alphanumeric and '\_'. Format: accessPolicies/{policy\_id}/accessLevels/{short\_name}
- 
- **description** - (Optional) Description of the AccessLevel and its use. Does not affect behavior.
  - **basic** - (Optional) A set of predefined conditions for the access level and a combining function. Structure is documented below.

The **basic** block supports:

- **combining\_function** - (Optional) How the conditions list should be combined to determine if a request is granted this AccessLevel. If AND is used, each Condition in conditions must be satisfied for the AccessLevel to be applied. If OR is used, at least one Condition in conditions must be satisfied for the AccessLevel to be applied. Defaults to AND if unspecified.
- **conditions** - (Required) A set of requirements for the AccessLevel to be granted. Structure is documented below.

The **conditions** block supports:

- **ip\_subnetworks** - (Optional) A list of CIDR block IP subnetwork specification. May be IPv4 or IPv6. Note that for a CIDR IP address block, the specified IP address portion must be properly truncated (i.e. all the host bits must be zero) or the input is considered malformed. For example, "192.0.2.0/24" is accepted but "192.0.2.1/24" is not. Similarly, for IPv6, "2001:db8::/32" is accepted whereas "2001:db8::1/32" is not. The originating IP of a request must be in one of the listed subnets in order for this Condition to be true. If empty, all IP addresses are allowed.
- **required\_access\_levels** - (Optional) A list of other access levels defined in the same Policy, referenced by resource name. Referencing an AccessLevel which does not exist is an error. All access levels listed must be granted for the Condition to be true. Format: `accessPolicies/{policy_id}/accessLevels/{short_name}`
- **members** - (Optional) An allowed list of members (users, groups, service accounts). The signed-in user originating the request must be a part of one of the provided members. If not specified, a request may come from any user (logged in/not logged in, not present in any groups, etc.). Formats: `user:{emailid}`, `group:{emailid}`, `serviceAccount:{emailid}`
- **negate** - (Optional) Whether to negate the Condition. If true, the Condition becomes a NAND over its non-empty fields, each field must be false for the Condition overall to be satisfied. Defaults to false.
- **device\_policy** - (Optional) Device specific restrictions, all restrictions must hold for the Condition to be true. If not specified, all devices are allowed. Structure is documented below.

The **device\_policy** block supports:

- **require\_screen\_lock** - (Optional) Whether or not screenlock is required for the DevicePolicy to be true. Defaults to false.
- **allowed\_encryption\_statuses** - (Optional) A list of allowed encryptions statuses. An empty list allows all statuses.
- **allowed\_device\_management\_levels** - (Optional) A list of allowed device management levels. An empty list allows all management levels.

- **os\_constraints** - (Optional) A list of allowed OS versions. An empty list allows all types and all versions. Structure is documented below.

The **os\_constraints** block supports:

- **minimum\_version** - (Optional) The minimum allowed OS version. If not set, any version of this OS satisfies the constraint. Format: "major.minor.patch" such as "10.5.301", "9.2.1".
- **os\_type** - (Optional) The operating system type of the device.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

AccessLevel can be imported using any of these accepted formats:

```
$ terraform import -provider=google-beta google_access_context_manager_access_level.default
```

If you're importing a resource with beta features, make sure to include **-provider=google-beta** as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_access\_\_context\_\_manager\_\_access\_\_policy

AccessPolicy is a container for AccessLevels (which define the necessary attributes to use GCP services) and ServicePerimeters (which define regions of services able to freely pass data within a perimeter). An access policy is globally visible within an organization, and the restrictions it specifies apply to all projects within an organization.

**Warning:** This resource is in beta, and should be used with the terraform-provider-google-beta provider. See Provider Versions for more details on beta resources.

To get more information about AccessPolicy, see:

- API documentation
- How-to Guides
  - Access Policy Quickstart

## » Example Usage - Access Context Manager Access Policy Basic

```
resource "google_access_context_manager_access_policy" "access-policy" {  
  parent = "organizations/123456789"  
  title  = "my policy"  
}
```

## » Argument Reference

The following arguments are supported:

- **parent** - (Required) The parent of this AccessPolicy in the Cloud Resource Hierarchy. Format: organizations/{organization\_id}
  - **title** - (Required) Human readable title. Does not affect behavior.
- 

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **name** - Resource name of the AccessPolicy. Format: {policy\_id}
- **create\_time** - Time the AccessPolicy was created in UTC.
- **update\_time** - Time the AccessPolicy was updated in UTC.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

AccessPolicy can be imported using any of these accepted formats:

```
$ terraform import -provider=google-beta google_access_context_manager_access_policy.default
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_access\_\_context\_\_manager\_\_service\_\_perimeter

ServicePerimeter describes a set of GCP resources which can freely import and export data amongst themselves, but not export outside of the ServicePerimeter. If a request with a source within this ServicePerimeter has a target outside of the ServicePerimeter, the request will be blocked. Otherwise the request is allowed. There are two types of Service Perimeter - Regular and Bridge. Regular Service Perimeters cannot overlap, a single GCP project can only belong to a single regular Service Perimeter. Service Perimeter Bridges can contain only GCP projects as members, a single GCP project may belong to multiple Service Perimeter Bridges.

**Warning:** This resource is in beta, and should be used with the terraform-provider-google-beta provider. See Provider Versions for more details on beta resources.

To get more information about ServicePerimeter, see:

- API documentation
- How-to Guides
  - Access Policy Quickstart

## » Example Usage - Access Context Manager Service Perimeter Basic

```
resource "google_access_context_manager_service_perimeter" "service-perimeter" {
  parent      = "accessPolicies/${google_access_context_manager_access_policy.test-access.name}"
  name        = "accessPolicies/${google_access_context_manager_access_policy.test-access.name}"
  title       = "restrict_all"
  status {
    restricted_services = ["*"]
  }
}

resource "google_access_context_manager_access_level" "access-level" {
  parent      = "accessPolicies/${google_access_context_manager_access_policy.test-access.name}"
  name        = "accessPolicies/${google_access_context_manager_access_policy.test-access.name}"
  title       = "ios_no_lock"
  basic {
    conditions {
      device_policy {
        require_screen_lock = false
        os_constraints {
          os_type = "IOS"
        }
      }
    }
  }
}
```

```

    }
  }
}

resource "google_access_context_manager_access_policy" "access-policy" {
  parent = "organizations/123456789"
  title  = "my policy"
}

```

## » Argument Reference

The following arguments are supported:

- **title** - (Required) Human readable title. Must be unique within the Policy.
  - **parent** - (Required) The AccessPolicy this ServicePerimeter lives in. Format: accessPolicies/{policy\_id}
  - **name** - (Required) Resource name for the ServicePerimeter. The short\_name component must begin with a letter and only include alphanumeric and '\_'. Format: accessPolicies/{policy\_id}/servicePerimeters/{short\_name}
- 
- **description** - (Optional) Description of the ServicePerimeter and its use. Does not affect behavior.
  - **perimeter\_type** - (Optional) Specifies the type of the Perimeter. There are two types: regular and bridge. Regular Service Perimeter contains resources, access levels, and restricted/unrestricted services. Every resource can be in at most ONE regular Service Perimeter. In addition to being in a regular service perimeter, a resource can also be in zero or more perimeter bridges. A perimeter bridge only contains resources. Cross project operations are permitted if all effected resources share some perimeter (whether bridge or regular). Perimeter Bridge does not contain access levels or services: those are governed entirely by the regular perimeter that resource is in. Perimeter Bridges are typically useful when building more complex topologies with many independent perimeters that need to share some data with a common perimeter, but should not be able to share data among themselves.
  - **status** - (Optional) ServicePerimeter configuration. Specifies sets of resources, restricted/unrestricted services and access levels that determine perimeter content and boundaries. Structure is documented below.

The **status** block supports:

- **resources** - (Optional) A list of GCP resources that are inside of the service perimeter. Currently only projects are allowed. Format: projects/{project\_number}
- **access\_levels** - (Optional) A list of AccessLevel resource names that allow resources within the ServicePerimeter to be accessed from the internet. AccessLevels listed must be in the same policy as this ServicePerimeter. Referencing a nonexistent AccessLevel is a syntax error. If no AccessLevel names are listed, resources within the perimeter can only be accessed via GCP calls with request origins within the perimeter. For Service Perimeter Bridge, must be empty. Format: accessPolicies/{policy\_id}/accessLevels/{access\_level\_name}
- **unrestricted\_services** - (Optional) GCP services that are not subject to the Service Perimeter restrictions. May contain a list of services or a single wildcard ". For example, if logging.googleapis.com is unrestricted, users can access logs inside the perimeter as if the perimeter doesn't exist, and it also means VMs inside the perimeter can access logs outside the perimeter. The wildcard means that unless explicitly specified by "restrictedServices" list, any service is treated as unrestricted. One of the fields "restrictedServices", "unrestrictedServices" must contain a wildcard "", otherwise the Service Perimeter specification is invalid. It also means that both field being empty is invalid as well. "unrestrictedServices" can be empty if and only if "restrictedServices" list contains a "\*" wildcard.
- **restricted\_services** - (Optional) GCP services that are subject to the Service Perimeter restrictions. May contain a list of services or a single wildcard ". For example, if storage.googleapis.com is specified, access to the storage buckets inside the perimeter must meet the perimeter's access restrictions. Wildcard means that unless explicitly specified by "unrestrictedServices" list, any service is treated as restricted. One of the fields "restrictedServices", "unrestrictedServices" must contain a wildcard "", otherwise the Service Perimeter specification is invalid. It also means that both field being empty is invalid as well. "restrictedServices" can be empty if and only if "unrestrictedServices" list contains a "\*" wildcard.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **create\_time** - Time the AccessPolicy was created in UTC.
- **update\_time** - Time the AccessPolicy was updated in UTC.



## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

ServicePerimeter can be imported using any of these accepted formats:

```
$ terraform import -provider=google-beta google_access_context_manager_service_perimeter.default
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_app\_engine\_application

Allows creation and management of an App Engine application.

App Engine applications cannot be deleted once they're created; you have to delete the entire project to delete the application. Terraform will report the application has been successfully deleted; this is a limitation of Terraform, and will go away in the future. Terraform is not able to delete App Engine applications.

## » Example Usage

```
resource "google_project" "my_project" {
  name      = "My Project"
  project_id = "your-project-id"
  org_id    = "1234567"
}

resource "google_app_engine_application" "app" {
  project      = "${google_project.my_project.project_id}"
  location_id = "us-central"
}
```

## » Argument Reference

The following arguments are supported:

- `location_id` - (Required) The location to serve the app from.
- `auth_domain` - (Optional) The domain to authenticate users with when using App Engine's User API.
- `serving_status` - (Optional) The serving status of the app.
- `feature_settings` - (Optional) A block of optional settings to configure specific App Engine features:
  - `split_health_checks` - (Optional) Set to false to use the legacy health check instead of the readiness and liveness checks.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `name` - Unique name of the app, usually `apps/{PROJECT_ID}`
- `url_dispatch_rule` - A list of dispatch rule blocks. Each block has a `domain`, `path`, and `service` field.
- `code_bucket` - The GCS bucket code is being stored in for this app.
- `default_hostname` - The default hostname for this app.
- `default_bucket` - The GCS bucket content is being stored in for this app.
- `gcr_domain` - The GCR domain used for storing managed Docker images for this app.

## » Import

Applications can be imported using the ID of the project the application belongs to, e.g.

```
$ terraform import google_app_engine_application.app your-project-id
```

## » `google_app_engine_firewall_rule`

A single firewall rule that is evaluated against incoming traffic and provides an action to take on matched requests.

To get more information about `FirewallRule`, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - App Engine Firewall Rule Basic

```
resource "google_project" "my_project" {
  name      = "tf-test-project"
  project_id = "test-project"
  org_id    = "123456789"
}

resource "google_app_engine_application" "app" {
  project      = "${google_project.my_project.project_id}"
  location_id = "us-central"
}

resource "google_app_engine_firewall_rule" "rule" {
  project = "${google_app_engine_application.app.project}"
  priority = 1000
  action = "ALLOW"
  source_range = "*"
}
```

## » Argument Reference

The following arguments are supported:

- **source\_range** - (Required) IP address or range, defined using CIDR notation, of requests that this rule applies to.
  - **action** - (Required) The action to take if this rule matches.
- 
- **description** - (Optional) An optional string description of this rule.
  - **priority** - (Optional) A positive integer that defines the order of rule evaluation. Rules with the lowest priority are evaluated first. A default rule at priority `Int32.MaxValue` matches all IPv4 and IPv6 traffic when no previous rule matches. Only the action of this rule can be modified by the user.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

FirewallRule can be imported using any of these accepted formats:

```
$ terraform import google_app_engine_firewall_rule.default {{project}}/{{priority}}
$ terraform import google_app_engine_firewall_rule.default {{priority}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_bigquery\_\_dataset

Creates a dataset resource for Google BigQuery. For more information see the official documentation and API.

## » Example Usage

```
resource "google_bigquery_dataset" "default" {
  dataset_id          = "foo"
  friendly_name       = "test"
  description         = "This is a test description"
  location            = "EU"
  default_table_expiration_ms = 3600000

  labels = {
    env = "default"
  }

  access {
    role   = "READER"
    domain = "example.com"
  }

  access {
    role           = "WRITER"
    group_by_email = "writers@example.com"
  }
}
```

```
}  
}
```

## » Argument Reference

The following arguments are supported:

- **dataset\_id** - (Required) A unique ID for the resource. Changing this forces a new resource to be created.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **friendly\_name** - (Optional) A descriptive name for the dataset.
- **description** - (Optional) A user-friendly description of the dataset.
- **delete\_contents\_on\_destroy** - (Optional) If set to `true`, delete all the tables in the dataset when destroying the resource; otherwise, destroying the resource will fail if tables are present.
- **location** - (Optional) The geographic location where the dataset should reside. See official docs.

There are two types of locations, regional or multi-regional. A regional location is a specific geographic place, such as Tokyo, and a multi-regional location is a large geographic area, such as the United States, that contains at least two geographic places

Possible regional values include: `asia-east1`, `asia-northeast1`, `asia-southeast1`, `australia-southeast1`, `europa-north1`, `europa-west2` and `us-east4`.

Possible multi-regional values: `EU` and `US`.

The default value is multi-regional location `US`. Changing this forces a new resource to be created.

- **default\_partition\_expiration\_ms** - (Optional) The default partition expiration for all partitioned tables in the dataset, in milliseconds.

Once this property is set, all newly-created partitioned tables in the dataset will have an `expirationMs` property in the `timePartitioning` settings set to this value, and changing the value will only affect new tables, not existing ones. The storage in a partition will have an expiration time of its partition time plus this value. Setting this property overrides the use of `defaultTableExpirationMs` for partitioned tables: only one of `defaultTableExpirationMs` and `defaultPartitionExpirationMs` will be used for any new partitioned table. If you provide an explicit

`timePartitioning.expirationMs` when creating or updating a partitioned table, that value takes precedence over the default partition expiration time indicated by this property.

- **default\_table\_expiration\_ms** - (Optional) The default lifetime of all tables in the dataset, in milliseconds. The minimum value is 3600000 milliseconds (one hour).

Once this property is set, all newly-created tables in the dataset will have an `expirationTime` property set to the creation time plus the value in this property, and changing the value will only affect new tables, not existing ones. When the `expirationTime` for a given table is reached, that table will be deleted automatically. If a table's `expirationTime` is modified or removed before the table expires, or if you provide an explicit `expirationTime` when creating a table, that value takes precedence over the default expiration time indicated by this property.

- **labels** - (Optional) A mapping of labels to assign to the resource.
- **access** - (Optional) An array of objects that define dataset access for one or more entities. Structure is documented below.

The **access** block supports the following fields (exactly one of **domain**, **group\_by\_email**, **special\_group**, **user\_by\_email**, or **view** must be set, even though they are marked optional):

- **role** - (Required unless **view** is set) Describes the rights granted to the user specified by the other member of the access object. The following string values are supported: **READER**, **WRITER**, **OWNER**.
- **domain** - (Optional) A domain to grant access to.
- **group\_by\_email** - (Optional) An email address of a Google Group to grant access to.
- **special\_group** - (Optional) A special group to grant access to. Possible values include:
  - **projectOwners**: Owners of the enclosing project.
  - **projectReaders**: Readers of the enclosing project.
  - **projectWriters**: Writers of the enclosing project.
  - **allAuthenticatedUsers**: All authenticated BigQuery users.
- **user\_by\_email** - (Optional) An email address of a user to grant access to.
- **view** - (Optional) A view from a different dataset to grant access to. Queries executed against that view will have read access to tables in this dataset. The **role** field is not required when this field is set. If that view is updated by any user, access to the view needs to be granted again via an update operation. Structure is documented below.

The `access.view` block supports:

- `dataset_id` - (Required) The ID of the dataset containing this table.
- `project_id` - (Required) The ID of the project containing this table.
- `table_id` - (Required) The ID of the table.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `self_link` - The URI of the created resource.
- `etag` - A hash of the resource.
- `creation_time` - The time when this dataset was created, in milliseconds since the epoch.
- `last_modified_time` - The date when this dataset or any of its tables was last modified, in milliseconds since the epoch.

## » Import

BigQuery datasets can be imported using the `project` and `dataset_id`, e.g.

```
$ terraform import google_bigquery_dataset.default gcp-project:foo
```

## » google\_\_bigquery\_\_table

Creates a table resource in a dataset for Google BigQuery. For more information see the official documentation and API.

## » Example Usage

```
resource "google_bigquery_dataset" "default" {
  dataset_id           = "foo"
  friendly_name        = "test"
  description          = "This is a test description"
  location             = "EU"
  default_table_expiration_ms = 3600000

  labels = {
    env = "default"
  }
}
```

```

    }
  }

  resource "google_bigquery_table" "default" {
    dataset_id = "${google_bigquery_dataset.default.dataset_id}"
    table_id   = "bar"

    time_partitioning {
      type = "DAY"
    }

    labels = {
      env = "default"
    }

    schema = "${file("schema.json")}"
  }

```

## » Argument Reference

The following arguments are supported:

- **dataset\_id** - (Required) The dataset ID to create the table in. Changing this forces a new resource to be created.
- **table\_id** - (Required) A unique ID for the resource. Changing this forces a new resource to be created.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **description** - (Optional) The field description.
- **expiration\_time** - (Optional) The time when this table expires, in milliseconds since the epoch. If not present, the table will persist indefinitely. Expired tables will be deleted and their storage reclaimed.
- **friendly\_name** - (Optional) A descriptive name for the table.
- **labels** - (Optional) A mapping of labels to assign to the resource.
- **schema** - (Optional) A JSON schema for the table.
- **time\_partitioning** - (Optional) If specified, configures time-based partitioning for this table. Structure is documented below.
- **view** - (Optional) If specified, configures this table as a view. Structure is documented below.

The `time_partitioning` block supports:



- **expiration\_ms** - (Optional) Number of milliseconds for which to keep the storage for a partition.
- **field** - (Optional) The field used to determine how to create a time-based partition. If time-based partitioning is enabled without this value, the table is partitioned based on the load time.
- **type** - (Required) The only type supported is DAY, which will generate one partition per day based on data loading time.
- **require\_partition\_filter** - (Optional) If set to true, queries over this table require a partition filter that can be used for partition elimination to be specified.

The **view** block supports:

- **query** - (Required) A query that BigQuery executes when the view is referenced.
- **use\_legacy\_sql** - (Optional) Specifies whether to use BigQuery's legacy SQL for this view. The default value is true. If set to false, the view will use BigQuery's standard SQL.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_time** - The time when this table was created, in milliseconds since the epoch.
- **etag** - A hash of the resource.
- **last\_modified\_time** - The time when this table was last modified, in milliseconds since the epoch.
- **location** - The geographic location where the table resides. This value is inherited from the dataset.
- **num\_bytes** - The size of this table in bytes, excluding any data in the streaming buffer.
- **num\_long\_term\_bytes** - The number of bytes in the table that are considered "long-term storage".
- **num\_rows** - The number of rows of data in this table, excluding any data in the streaming buffer.
- **self\_link** - The URI of the created resource.
- **type** - Describes the table type.

## » Import

BigQuery tables can be imported using the `project`, `dataset_id`, and `table_id`, e.g.

```
$ terraform import google_bigquery_table.default gcp-project:foo.bar
```

## » google\_\_bigtable\_\_instance

Creates a Google Bigtable instance. For more information see the official documentation and API.

### » Example Usage - Production Instance

```
resource "google_bigtable_instance" "production-instance" {
  name = "tf-instance"

  cluster {
    cluster_id = "tf-instance-cluster"
    zone       = "us-central1-b"
    num_nodes  = 3
    storage_type = "HDD"
  }
}
```

### » Example Usage - Development Instance

```
resource "google_bigtable_instance" "development-instance" {
  name = "tf-instance"
  instance_type = "DEVELOPMENT"

  cluster {
    cluster_id = "tf-instance-cluster"
    zone       = "us-central1-b"
    storage_type = "HDD"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name (also called Instance Id in the Cloud Console) of the Cloud Bigtable instance.
- **cluster** - (Required) A block of cluster configuration options. This can be specified 1 or 2 times. See structure below.

- 
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
  - **instance\_type** - (Optional) The instance type to create. One of "DEVELOPMENT" or "PRODUCTION". Defaults to "PRODUCTION".
  - **display\_name** - (Optional) The human-readable display name of the Bigtable instance. Defaults to the instance **name**.
- 

The **cluster** block supports the following arguments:

- **cluster\_id** - (Required) The ID of the Cloud Bigtable cluster.
- **zone** - (Required) The zone to create the Cloud Bigtable cluster in. Each cluster must have a different zone in the same region. Zones that support Bigtable instances are noted on the Cloud Bigtable locations page.
- **num\_nodes** - (Optional) The number of nodes in your Cloud Bigtable cluster. Required, with a minimum of 3 for a **PRODUCTION** instance. Must be left unset for a **DEVELOPMENT** instance.
- **storage\_type** - (Optional) The storage type to use. One of "SSD" or "HDD". Defaults to "SSD".

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » google\_\_bigtable\_\_table

Creates a Google Cloud Bigtable table inside an instance. For more information see the official documentation and API.

## » Example Usage

```
resource "google_bigtable_instance" "instance" {
  name          = "tf-instance"
  cluster_id    = "tf-instance-cluster"
```

```

zone          = "us-central1-b"
num_nodes     = 3
storage_type  = "HDD"
}

resource "google_bigtable_table" "table" {
  name          = "tf-table"
  instance_name = "${google_bigtable_instance.instance.name}"
  split_keys    = ["a", "b", "c"]
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the table.
- **instance\_name** - (Required) The name of the Bigtable instance.
- **split\_keys** - (Optional) A list of predefined keys to split the table on.
- **column\_family** - (Optional) A group of columns within a table which share a common configuration. This can be specified multiple times. Structure is documented below.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

---

**column\_family** supports the following arguments:

- **family** - (Optional) The name of the column family.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » google\_\_binary\_\_authorization\_\_attestor

An attestor that attests to container image artifacts.

**Warning:** This resource is in beta, and should be used with the terraform-provider-google-beta provider. See Provider Versions for more details on beta resources.

To get more information about Attestor, see:

- API documentation
- How-to Guides
  - Official Documentation

## » Example Usage - Binary Authorization Attestor Basic

```
resource "google_binary_authorization_attestor" "attestor" {
  name = "test-attestor"
  attestation_authority_note {
    note_reference = "${google_container_analysis_note.note.name}"
    public_keys {
      ascii_armored_pgp_public_key = <<EOF
mqENBFtP0doBCADF+joTiXWKVuP8kJt3fgpBSjT9h8ezMfKA4aXZctYLx5ws1WQl
bB7Iu2ezkECNzoEeU7WxUe8a61pMCh9cisS9H5mB2K2uM4Jnf8tgFeXn3akJDVo0
oR1IC+Dp9mXbRSK3MAvKkOwWlG99sx3uEdvmeBRHB00+grchLx24EThXF0yP9Fk6
V39j6xMjw4aggLD15B4V0v9JqBDdJiIYFzszZDL6pJwZrzcP0z8JO4rTZd+f64bD
Mpj52j/pQfA81ZH0aAgb1OrthLdMrBAjoDjArV4Ek7vSbrcgYWcI6BhsQrFoxKdX
83TZKai55ZCfCLIskwUIzA1NLVwyzCS+fSN/ABEBAAGOKCJUZXNOIEF0dGVzdG9y
IiA8ZGFuYWVhZmZtYW5AZZ29vZ2x1LmNvbT6JAU4EEwEiADgWIQRfWkqHt6hpTA1L
uY060eeM4dc66AUCW0/R2gIbLwULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRA6
0eeM4dc66HdpCAC4ot3b00yxPb0Ip+WT2U0PbpTBPJklesuwpIrM4Lh0N+1nVRLC
51WSmVbM8BiAFhLbN9LpdHhds1kUrHF7+wWAjdR8sqAj9otc6HGRM/3qfa2qgh+U
WTEk/3us/rYSi7T7TkMuutRMia1IkR13uKiW56csEMnb0Qpn9rDqwIr5R8n1ZP5h
MAU9vdm1D1v567meMqTaVZgR3w7bck2P49A08105ERFpVkErtu/98y+rUy9d789l
+OPuS1NGnxI1YKsNaWJF4uJVuvQuZ1twrhCbGNtVor02U12+cEq+YtUxj7kmd0C1
qoIRW6y0+U1Ac+MbqfL0ziHD0Amcqz1GnR0g
=6Bvm
EOF
    }
  }
}

resource "google_container_analysis_note" "note" {
  name = "test-attestor-note"
  attestation_authority {
    hint {
      human_readable_name = "Attestor Note"
    }
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The resource name.
- **attestation\_authority\_note** - (Required) A Container Analysis ATTESTATION\_AUTHORITY Note, created by the user. Structure is documented below.

The **attestation\_authority\_note** block supports:

- **note\_reference** - (Required) The resource name of a ATTESTATION\_AUTHORITY Note, created by the user. If the Note is in a different project from the Attestor, it should be specified in the format **projects/\*/notes/\*** (or the legacy **providers/\*/notes/\***). This field may not be updated. An attestation by this attestor is stored as a Container Analysis ATTESTATION\_AUTHORITY Occurrence that names a container image and that links to this Note.
- **public\_keys** - (Optional) Public keys that verify attestations signed by this attestor. This field may be updated. If this field is non-empty, one of the specified public keys must verify that an attestation was signed by this attestor for the image specified in the admission request. If this field is empty, this attestor always returns that no valid attestations exist. Structure is documented below.
- **delegation\_service\_account\_email** - This field will contain the service account email address that this Attestor will use as the principal when querying Container Analysis. Attestor administrators must grant this service account the IAM role needed to read attestations from the `noteReference` in Container Analysis (`containeranalysis.notes.occurrences.viewer`). This email address is fixed for the lifetime of the Attestor, but callers should not make any other assumptions about the service account email; future versions may use an email based on a different naming pattern.

The **public\_keys** block supports:

- **comment** - (Optional) A descriptive comment. This field may be updated.
  - **id** - This field will be overwritten with key ID information, for example, an identifier extracted from a PGP public key. This field may not be updated.
  - **ascii\_armored\_pgp\_public\_key** - (Required) ASCII-armored representation of a PGP public key, as the entire output by the command `gpg --export --armor foo@example.com` (either LF or CRLF line endings).
- 
- **description** - (Optional) A descriptive comment. This field may be updated. The field may be displayed in chooser dialogs.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Attestor can be imported using any of these accepted formats:

```
$ terraform import -provider=google-beta google_binary_authorization_attestor.default projec
$ terraform import -provider=google-beta google_binary_authorization_attestor.default {{proj
$ terraform import -provider=google-beta google_binary_authorization_attestor.default {{name
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_binary\_\_authorization\_\_policy

A policy for container image binary authorization.

**Warning:** This resource is in beta, and should be used with the `terraform-provider-google-beta` provider. See [Provider Versions](#) for more details on beta resources.

To get more information about Policy, see:

- [API documentation](#)
- [How-to Guides](#)
  - [Official Documentation](#)

## » Example Usage - Binary Authorization Policy Basic

```
resource "google_binary_authorization_policy" "policy" {
  admission_whitelist_patterns {
    name_pattern= "gcr.io/google_containers/*"
  }

  default_admission_rule {
    evaluation_mode = "ALWAYS_ALLOW"
    enforcement_mode = "ENFORCED_BLOCK_AND_AUDIT_LOG"
  }
}
```

```

cluster_admission_rules {
  cluster = "us-central1-a.prod-cluster"
  evaluation_mode = "REQUIRE_ATTESTATION"
  enforcement_mode = "ENFORCED_BLOCK_AND_AUDIT_LOG"
  require_attestations_by = ["${google_binary_authorization_attestor.attestor.name}"]
}

resource "google_container_analysis_note" "note" {
  name = "test-attestor-note"
  attestation_authority {
    hint {
      human_readable_name = "My attestor"
    }
  }
}

resource "google_binary_authorization_attestor" "attestor" {
  name = "test-attestor"
  attestation_authority_note {
    note_reference = "${google_container_analysis_note.note.name}"
  }
}

```

## » Argument Reference

The following arguments are supported:

- **default\_admission\_rule** - (Required) Default admission rule for a cluster without a per-cluster admission rule. Structure is documented below.

The **default\_admission\_rule** block supports:

- **evaluation\_mode** - (Required) How this admission rule will be evaluated.
- **require\_attestations\_by** - (Optional) The resource names of the attestors that must attest to a container image. If the attestor is in a different project from the policy, it should be specified in the format **projects/\*/attestors/\***. Each attestor must exist before a policy can reference it. To add an attestor to a policy the principal issuing the policy change request must be able to read the attestor resource. Note: this field must be non-empty when the **evaluation\_mode** field specifies **REQUIRE\_ATTESTATION**, otherwise it must be empty.
- **enforcement\_mode** - (Required) The action when a pod creation is denied by the admission rule.



- 
- **description** - (Optional) A descriptive comment.
  - **admission\_whitelist\_patterns** - (Optional) A whitelist of image patterns to exclude from admission rules. If an image's name matches a whitelist pattern, the image's admission requests will always be permitted regardless of your admission rules. Structure is documented below.
  - **cluster\_admission\_rules** - (Optional) Per-cluster admission rules. An admission rule specifies either that all container images used in a pod creation request must be attested to by one or more attestors, that all pod creations will be allowed, or that all pod creations will be denied. There can be at most one admission rule per cluster spec.

Identifier format: `{{location}}.{{clusterId}}`. A location is either a compute zone (e.g. `us-central1-a`) or a region (e.g. `us-central1`). Structure is documented below. \* **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **admission\_whitelist\_patterns** block supports:

- **name\_pattern** - (Optional) An image name pattern to whitelist, in the form `registry/path/to/image`. This supports a trailing `*` as a wildcard, but this is allowed only in text after the `registry/` part.

The **cluster\_admission\_rules** block supports:

- **cluster** - (Required) The identifier for this object. Format specified above.
- **evaluation\_mode** - (Optional) How this admission rule will be evaluated.
- **require\_attestations\_by** - (Optional) The resource names of the attestors that must attest to a container image. If the attestor is in a different project from the policy, it should be specified in the format `projects/*/attestors/*`. Each attestor must exist before a policy can reference it. To add an attestor to a policy the principal issuing the policy change request must be able to read the attestor resource. Note: this field must be non-empty when the `evaluation_mode` field specifies `REQUIRE_ATTESTATION`, otherwise it must be empty.
- **enforcement\_mode** - (Optional) The action when a pod creation is denied by the admission rule.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.

- `delete` - Default is 4 minutes.

## » Import

Policy can be imported using any of these accepted formats:

```
$ terraform import -provider=google-beta google_binary_authorization_policy.default projects
$ terraform import -provider=google-beta google_binary_authorization_policy.default {{project_id}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_cloudbuild_trigger`

Configuration for an automated build in response to source repository changes.

To get more information about Trigger, see:

- API documentation
- How-to Guides
  - Automating builds using build triggers



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Cloudbuild Trigger Filename

```
resource "google_cloudbuild_trigger" "filename-trigger" {
  trigger_template {
    branch_name = "master"
    repo_name   = "my-repo"
  }

  substitutions = {
    _FOO = "bar"
    _BAZ = "qux"
  }

  filename = "cloudbuild.yaml"
}
```

## » Argument Reference

The following arguments are supported:

- 
- **description** - (Optional) Human-readable description of the trigger.
  - **disabled** - (Optional) Whether the trigger is disabled or not. If true, the trigger will never result in a build.
  - **substitutions** - (Optional) Substitutions data for Build resource.
  - **filename** - (Optional) Path, from the source root, to a file whose contents is used for the template. Either a filename or build template must be provided.
  - **ignored\_files** - (Optional) ignoredFiles and includedFiles are file glob matches using `http://godoc/pkg/path/filepath#Match` extended with support for `**`. If ignoredFiles and changed files are both empty, then they are not used to determine whether or not to trigger a build. If ignoredFiles is not empty, then we ignore any files that match any of the ignored\_file globs. If the change has no files that are outside of the ignoredFiles globs, then we do not trigger a build.
  - **included\_files** - (Optional) ignoredFiles and includedFiles are file glob matches using `http://godoc/pkg/path/filepath#Match` extended with support for `**`. If any of the files altered in the commit pass the ignoredFiles filter and includedFiles is empty, then as far as this filter is concerned, we should trigger the build. If any of the files altered in the commit pass the ignoredFiles filter and includedFiles is not empty, then we make sure that at least one of those files matches a includedFiles glob. If not, then we do not trigger a build.
  - **trigger\_template** - (Optional) Template describing the types of source changes to trigger a build. Branch and tag names in trigger templates are interpreted as regular expressions. Any branch or tag change that matches that regular expression will trigger a build. Structure is documented below.
  - **build** - (Optional) Contents of the build template. Either a filename or build template must be provided. Structure is documented below.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **trigger\_template** block supports:

- **project\_id** - (Optional) ID of the project that owns the Cloud Source Repository. If omitted, the project ID requesting the build is assumed.

- **repo\_name** - (Optional) Name of the Cloud Source Repository. If omitted, the name "default" is assumed.
- **dir** - (Optional) Directory, relative to the source root, in which to run the build. This must be a relative path. If a step's dir is specified and is an absolute path, this value is ignored for that step's execution.
- **branch\_name** - (Optional) Name of the branch to build. Exactly one of a branch name, tag, or commit SHA must be provided.
- **tag\_name** - (Optional) Name of the tag to build. Exactly one of a branch name, tag, or commit SHA must be provided.
- **commit\_sha** - (Optional) Explicit commit SHA to build. Exactly one of a branch name, tag, or commit SHA must be provided.

The **build** block supports:

- **tags** - (Optional) Tags for annotation of a Build. These are not docker tags.
- **images** - (Optional) A list of images to be pushed upon the successful completion of all build steps. The images are pushed using the builder service account's credentials. The digests of the pushed images will be stored in the Build resource's results field. If any of the images fail to be pushed, the build status is marked FAILURE.
- **step** - (Optional) The operations to be performed on the workspace. Structure is documented below.

The **step** block supports:

- **name** - (Optional) The name of the container image that will run this particular build step. If the image is available in the host's Docker daemon's cache, it will be run directly. If not, the host will attempt to pull the image first, using the builder service account's credentials if necessary. The Docker daemon's cache will already have the latest versions of all of the officially supported build steps (<https://github.com/GoogleCloudPlatform/cloud-builders>). The Docker daemon will also have cached many of the layers for some popular images, like "ubuntu", "debian", but they will be refreshed at the time you attempt to use them. If you built an image in a previous build step, it will be stored in the host's Docker daemon's cache and is available to use as the name for a later build step.
- **args** - (Optional) A list of arguments that will be presented to the step when it is started. If the image used to run the step's container has an entrypoint, the args are used as arguments to that entrypoint. If the image does not define an entrypoint, the first element in args is used as the entrypoint, and the remainder will be used as arguments.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `trigger_id` - The unique identifier for the trigger.
- `create_time` - Time when the trigger was created.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Trigger can be imported using any of these accepted formats:

```
$ terraform import google_cloudbuild_trigger.default projects/{{project}}/triggers/{{trigger_id}}
$ terraform import google_cloudbuild_trigger.default {{project}}/{{trigger_id}}
$ terraform import google_cloudbuild_trigger.default {{trigger_id}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_composer_environment`

An environment for running orchestration tasks.

Environments run Apache Airflow software on Google infrastructure.

To get more information about Environments, see:

- API documentation
- How-to Guides
  - Official Documentation
  - Configuring Shared VPC for Composer Environments
- Apache Airflow Documentation

**Warning:** We **STRONGLY** recommend you read the GCP guides as the Environment resource requires a long deployment process and involves several layers of GCP infrastructure, including a Kubernetes Engine cluster, Cloud Storage, and Compute networking resources. Due to limitations of the API, Terraform

will not be able to automatically find or manage many of these underlying resources. In particular: \* It can take up to one hour to create or update an environment resource. In addition, GCP may only detect some errors in configuration when they are used (e.g. ~40-50 minutes into the creation process), and is prone to limited error reporting. If you encounter confusing or uninformative errors, please verify your configuration is valid against GCP Cloud Composer before filing bugs against the Terraform provider. \* **Environments create Google Cloud Storage buckets that do not get cleaned up automatically** on environment deletion. More about Composer's use of Cloud Storage.

## » Example Usage

### » Basic Usage

```
resource "google_composer_environment" "test" {
  name     = "my-composer-env"
  region   = "us-central1"
}
```

### » With GKE and Compute Resource Dependencies

**NOTE** To use service accounts, you need to give `role/composer.worker` to the service account on any resources that may be created for the environment (i.e. at a project level). This will probably require an explicit dependency on the IAM policy binding (see `google_project_iam_member` below).

```
resource "google_composer_environment" "test" {
  name     = "%s"
  region   = "us-central1"
  config {
    node_count = 4

    node_config {
      zone = "us-central1-a"
      machine_type = "n1-standard-1"

      network = "${google_compute_network.test.self_link}"
      subnetwork = "${google_compute_subnetwork.test.self_link}"

      service_account = "${google_service_account.test.name}"
    }
  }
}
```

```

    depends_on = ["google_project_iam_member.composer-worker"]
}

resource "google_compute_network" "test" {
  name          = "composer-test-network"
  auto_create_subnetworks = false
}

resource "google_compute_subnetwork" "test" {
  name          = "composer-test-subnetwork"
  ip_cidr_range = "10.2.0.0/16"
  region        = "us-central1"
  network       = "${google_compute_network.test.self_link}"
}

resource "google_service_account" "test" {
  account_id = "composer-env-account"
  display_name = "Test Service Account for Composer Environment"
}

resource "google_project_iam_member" "composer-worker" {
  role    = "roles/composer.worker"
  member  = "serviceAccount:${google_service_account.test.email}"
}

```

## » With Software (Airflow) Config

```

resource "google_composer_environment" "test" {
  name = "%s"
  region = "us-central1"

  config {
    software_config {
      airflow_config_overrides = {
        core-load_example = "True"
      }

      pypi_packages = {
        numpy = ""
        scipy = "==1.1.0"
      }

      env_variables = {
        FOO = "bar"
      }
    }
  }
}

```

```

    }
  }
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the environment
- 
- **config** - (Optional) Configuration parameters for this environment Structure is documented below.
  - **labels** - (Optional) User-defined labels for this environment. The labels map can contain no more than 64 entries. Entries of the labels map are UTF8 strings that comply with the following restrictions: Label keys must be between 1 and 63 characters long and must conform to the following regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?`. Label values must be between 0 and 63 characters long and must conform to the regular expression `([a-z]([-a-z0-9]*[a-z0-9])?)?`. No more than 64 labels can be associated with a given environment. Both keys and values must be  $\leq 128$  bytes in size.
  - **region** - (Optional) The location or Compute Engine region for the environment.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **config** block supports:

- **node\_count** - (Optional) The number of nodes in the Kubernetes Engine cluster that will be used to run this environment.
- **node\_config** - (Optional) The configuration used for the Kubernetes Engine cluster. Structure is documented below.
- **software\_config** - (Optional) The configuration settings for software inside the environment. Structure is documented below.

The **node\_config** block supports:

- **zone** - (Required) The Compute Engine zone in which to deploy the VMs running the Apache Airflow software, specified as the zone name or relative resource name (e.g. `"projects/{project}/zones/{zone}"`). Must belong to the enclosing environment's project and region.



- **machine\_type** - (Optional) The Compute Engine machine type used for cluster instances, specified as a name or relative resource name. For example: "projects/{project}/zones/{zone}/machineTypes/{machineType}". Must belong to the enclosing environment's project and region/zone.
- **network** - (Optional) The Compute Engine network to be used for machine communications, specified as a self-link, relative resource name (e.g. "projects/{project}/global/networks/{network}"), by name.

The network must belong to the environment's project. If unspecified, the "default" network ID in the environment's project is used. If a Custom Subnet Network is provided, subnetwork must also be provided.

- **subnetwork** - (Optional) The Compute Engine subnetwork to be used for machine communications, , specified as a self-link, relative resource name (e.g. "projects/{project}/regions/{region}/subnetworks/{subnetwork}"), or by name. If subnetwork is provided, network must also be provided and the subnetwork must belong to the enclosing environment's project and region.
- **disk\_size\_gb** - (Optional) The disk size in GB used for node VMs. Minimum size is 20GB. If unspecified, defaults to 100GB. Cannot be updated.
- **oauth\_scopes** - (Optional) The set of Google API scopes to be made available on all node VMs. Cannot be updated. If empty, defaults to ["https://www.googleapis.com/auth/cloud-platform"]
- **service\_account** - (Optional) The Google Cloud Platform Service Account to be used by the node VMs. If a service account is not specified, the "default" Compute Engine service account is used. Cannot be updated. If given, note that the service account must have **roles/composer.worker** for any GCP resources created under the Cloud Composer Environment.
- **tags** - (Optional) The list of instance tags applied to all node VMs. Tags are used to identify valid sources or targets for network firewalls. Each tag within the list must comply with RFC1035. Cannot be updated.

The **software\_config** block supports:

- **airflow\_config\_overrides** - (Optional) Apache Airflow configuration properties to override. Property keys contain the section and property names, separated by a hyphen, for example "core-dags\_are\_paused\_at\_creation".

Section names must not contain hyphens ("-"), opening square brackets ("["), or closing square brackets ("]"). The property name must not be empty and cannot contain "=" or ";". Section and property names cannot contain characters: ":" Apache Airflow configuration property names must be written in snake\_case. Property values can contain any character, and can be written in any lower/upper case format. Certain Apache Airflow configuration property values are blacklisted, and cannot be overridden.

- **pypi\_packages** - (Optional) Custom Python Package Index (PyPI) packages to be installed in the environment. Keys refer to the lowercase package name (e.g. "numpy"). Values are the lowercase extras and version specifier (e.g. "==1.12.0", "[devel,gcp\_api]", "[devel]>=1.8.2, <1.9.2"). To specify a package without pinning it to a version specifier, use the empty string as the value.
- **env\_variables** - (Optional) Additional environment variables to provide to the Apache Airflow scheduler, worker, and webserver processes. Environment variable names must match the regular expression `[a-zA-Z][a-zA-Z0-9_]*`. They cannot specify Apache Airflow software configuration overrides (they cannot match the regular expression `AIRFLOW__[A-Z0-9_]+__[A-Z0-9_]+`), and they cannot match any of the following reserved names: `AIRFLOW_HOME C_FORCE_ROOT CONTAINER_NAME DAGS_FOLDER GCP_PROJECT GCS_BUCKET GKE_CLUSTER_NAME SQL_DATABASE SQL_INSTANCE SQL_PASSWORD SQL_PROJECT SQL_REGION SQL_USER`
- **image\_version** (Optional, Beta) - The version of the software running in the environment. This encapsulates both the version of Cloud Composer functionality and the version of Apache Airflow. It must match the regular expression `composer-[0-9]+\.[0-9]+(\.[0-9]+)?-airflow-[0-9]+\.[0-9]+(\.[0-9]+.*)?`. The Cloud Composer portion of the version is a semantic version. The portion of the image version following 'airflow-' is an official Apache Airflow repository release name. See documentation for allowed release names. This field can only be set in the Beta) provider, but is an output-only attribute in the GA provider.
- **python\_version** (Optional, Beta) - The major version of Python used to run the Apache Airflow scheduler, worker, and webserver processes. Can be set to '2' or '3'. If not specified, the default is '2'. Cannot be updated.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **config.gke\_cluster** - The Kubernetes Engine cluster used to run this environment.
- **config.dag\_gcs\_prefix** - The Cloud Storage prefix of the DAGs for this environment. Although Cloud Storage objects reside in a flat namespace, a hierarchical file tree can be simulated using '/'-delimited object name prefixes. DAG objects for this environment reside in a simulated directory with this prefix.
- **config.airflow\_uri** - The URI of the Apache Airflow Web UI hosted within this environment.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 60 minutes.
- `update` - Default is 60 minutes.
- `delete` - Default is 6 minutes.

## » Import

Environment can be imported using any of these accepted formats:

```
$ terraform import google_composer_environment.default projects/{{project}}/locations/{{region}}/{{environment}}
$ terraform import google_composer_environment.default {{project}}/{{region}}/{{name}}
$ terraform import google_composer_environment.default {{name}}
```

## » google\_cloudfunctions\_function

Creates a new Cloud Function. For more information see the official documentation and API.

## » Example Usage

```
resource "google_storage_bucket" "bucket" {
  name = "test-bucket"
}

resource "google_storage_bucket_object" "archive" {
  name     = "index.zip"
  bucket   = "${google_storage_bucket.bucket.name}"
  source   = "./path/to/zip/file/which/contains/code"
}

resource "google_cloudfunctions_function" "function" {
  name                = "function-test"
  description         = "My function"
  available_memory_mb = 128
  source_archive_bucket = "${google_storage_bucket.bucket.name}"
  source_archive_object = "${google_storage_bucket_object.archive.name}"
  trigger_http        = true
  timeout             = 60
  entry_point         = "helloGET"
  labels = {
```

```

    my-label = "my-label-value"
  }

  environment_variables = {
    MY_ENV_VAR = "my-env-var-value"
  }
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A user-defined name of the function. Function names must be unique globally.
- 
- **description** - (Optional) Description of the function.
  - **available\_memory\_mb** - (Optional) Memory (in MB), available to the function. Default value is 256MB. Allowed values are: 128MB, 256MB, 512MB, 1024MB, and 2048MB.
  - **timeout** - (Optional) Timeout (in seconds) for the function. Default value is 60 seconds. Cannot be more than 540 seconds.
  - **entry\_point** - (Optional) Name of the function that will be executed when the Google Cloud Function is triggered.
  - **event\_trigger** - (Optional) A source that fires events in response to a condition in another service. Structure is documented below. Cannot be used with `trigger_http`.
  - **trigger\_http** - (Optional) Boolean variable. Any HTTP request (of a supported type) to the endpoint will trigger function execution. Supported HTTP request types are: POST, PUT, GET, DELETE, and OPTIONS. Endpoint is returned as `https_trigger_url`. Cannot be used with `trigger_bucket` and `trigger_topic`.
  - **labels** - (Optional) A set of key/value label pairs to assign to the function.
  - **runtime** - (Optional) The runtime in which the function is going to run. If empty, defaults to "nodejs6".
  - **service\_account\_email** - (Optional) If provided, the self-provided service account to run the function with.
  - **environment\_variables** - (Optional) A set of key/value environment variable pairs to assign to the function.

- **source\_archive\_bucket** - (Optional) The GCS bucket containing the zip archive which contains the function.
- **source\_archive\_object** - (Optional) The source archive object (file) in archive bucket.
- **source\_repository** - (Optional) Represents parameters related to source repository where a function is hosted. Cannot be set alongside **source\_archive\_bucket** or **source\_archive\_object**. Structure is documented below.

The **event\_trigger** block supports:

- **event\_type** - (Required) The type of event to observe. For example: `"google.storage.object.finalize"`. See the documentation on calling Cloud Functions for a full reference. Cloud Storage, Cloud Pub/Sub and Cloud Firestore triggers are supported at this time. Legacy triggers are supported, such as `"providers/cloud.storage/eventTypes/object.change"`, `"providers/cloud.pubsub/eventTypes/topic.publish"` and `"providers/cloud.firestore/eventTypes/document.create"`.
- **resource** - (Required) Required. The name of the resource from which to observe events, for example, `"myBucket"`.
- **failure\_policy** - (Optional) Specifies policy for failed executions. Structure is documented below.

The **failure\_policy** block supports:

- **retry** - (Required) Whether the function should be retried on failure. Defaults to `false`.

The **source\_repository** block supports:

- **url** - (Required) The URL pointing to the hosted repository where the function is defined. There are supported Cloud Source Repository URLs in the following formats:
  - To refer to a specific commit: `https://source.developers.google.com/projects/*/repos/*/revisions/*`
  - To refer to a moveable alias (branch): `https://source.developers.google.com/projects/*/repos/*/aliases/*`. To refer to HEAD, use the `master` moveable alias.
  - To refer to a specific fixed alias (tag): `https://source.developers.google.com/projects/*/repos/*/aliases/*`

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **https\_trigger\_url** - URL which triggers function execution. Returned only if **trigger\_http** is used.

- `source_repository.0.deployed_url` - The URL pointing to the hosted repository where the function was defined at the time of deployment.
- `project` - Project of the function. If it is not provided, the provider project is used.
- `region` - Region of function. Currently can be only "us-central1". If it is not provided, the provider region is used.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 5 minutes.
- `update` - Default is 5 minutes.
- `delete` - Default is 5 minutes.

## » Import

Functions can be imported using the `name`, e.g.

```
$ terraform import google_cloudfunctions_function.default function-test
```

## » google\_billing\_account\_\_iam\_binding

Allows creation and management of a single binding within IAM policy for an existing Google Cloud Platform Billing Account.

**Note:** This resource **must not** be used in conjunction with `google_billing_account_iam_member` for the **same role** or they will fight over what your policy should be.

**Note:** On create, this resource will overwrite members of any existing roles. Use `terraform import` and inspect the `terraform plan` output to ensure your existing members are preserved.

## » Example Usage

```
resource "google_billing_account_iam_binding" "binding" {
  billing_account_id = "00AA00-000AAA-00AA0A"
  role               = "roles/billing.viewer"

  members = [
    "user:alice@gmail.com",
  ]
}
```

## » Argument Reference

The following arguments are supported:

- `billing_account_id` - (Required) The billing account id.
- `role` - (Required) The role that should be applied.
- `members` - (Required) A list of users that the role should apply to. For more details on format and restrictions see <https://cloud.google.com/billing/reference/rest/v1/Policy#Binding>

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `etag` - (Computed) The etag of the billing account's IAM policy.

## » Import

IAM binding imports use space-delimited identifiers; first the resource in question and then the role. These bindings can be imported using the `billing_account_id` and `role`, e.g.

```
$ terraform import google_billing_account_iam_binding.binding "your-billing-account-id roles"
```

## » `google_billing_account_iam_member`

Allows creation and management of a single member for a single binding within the IAM policy for an existing Google Cloud Platform Billing Account.

**Note:** This resource **must not** be used in conjunction with `google_billing_account_iam_binding` for the **same role** or they will fight over what your policy should be.

## » Example Usage

```
resource "google_billing_account_iam_member" "binding" {  
  billing_account_id = "00AA00-000AAA-00AA0A"  
  role               = "roles/billing.viewer"  
  member             = "user:alice@gmail.com"  
}
```

## » Argument Reference

The following arguments are supported:

- `billing_account_id` - (Required) The billing account id.
- `role` - (Required) The role that should be applied.
- `member` - (Required) The user that the role should apply to. For more details on format and restrictions see <https://cloud.google.com/billing/reference/rest/v1/Policy#Binding>

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `etag` - (Computed) The etag of the billing account's IAM policy.

## » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the `billing_account_id`, `role`, and `member` identity, e.g.

```
$ terraform import google_billing_account_iam_member.binding "your-billing-account-id roles"
```

## » `google_billing_account_iam_policy`

Allows management of the entire IAM policy for an existing Google Cloud Platform Billing Account.

**Warning:** Billing accounts have a default user that can be **overwritten** by use of this resource. The safest alternative is to use multiple `google_billing_account_iam_binding` resources. If you do use this resource, the best way to be sure that you are not making dangerous changes is to start by importing your existing policy, and examining the diff very closely.

**Note:** This resource **must not** be used in conjunction with `google_billing_account_iam_member` or `google_billing_account_iam_binding` or they will fight over what your policy should be.



## » Example Usage

```
resource "google_billing_account_iam_policy" "policy" {
  billing_account_id = "00AA00-000AAA-00AA0A"
  policy_data        = "${data.google_iam_policy.admin.policy_data}"
}

data "google_iam_policy" "admin" {
  binding {
    role = "roles/billing.viewer"

    members = [
      "user:jane@example.com",
    ]
  }
}
```

## » Argument Reference

The following arguments are supported:

- `billing_account_id` - (Required) The billing account id.
- `policy_data` - (Required) The `google_iam_policy` data source that represents the IAM policy that will be applied to the billing account. This policy overrides any existing policy applied to the billing account.

## » Import

```
$ terraform import google_billing_account_iam_policy.policy billing-account-id
```

## » google\_\_folder

Allows management of a Google Cloud Platform folder. For more information see the official documentation and API.

A folder can contain projects, other folders, or a combination of both. You can use folders to group projects under an organization in a hierarchy. For example, your organization might contain multiple departments, each with its own set of Cloud Platform resources. Folders allows you to group these resources on a per-department basis. Folders are used to group resources that share common IAM policies.

Folders created live inside an Organization. See the Organization documentation for more details.

The service account used to run Terraform when creating a `google_folder` resource must have `roles/resourcemanager.folderCreator`. See the Access Control for Folders Using IAM doc for more information.

## » Example Usage

```
# Top-level folder under an organization.
resource "google_folder" "department1" {
  display_name = "Department 1"
  parent      = "organizations/1234567"
}

# Folder nested under another folder.
resource "google_folder" "team-abc" {
  display_name = "Team ABC"
  parent      = "${google_folder.department1.name}"
}
```

## » Argument Reference

The following arguments are supported:

- `display_name` - (Required) The folder's display name. A folder's display name must be unique amongst its siblings, e.g. no two folders with the same parent can share the same display name. The display name must start and end with a letter or digit, may contain letters, digits, spaces, hyphens and underscores and can be no longer than 30 characters.
- `parent` - (Required) The resource name of the parent Folder or Organization. Must be of the form `folders/{folder_id}` or `organizations/{org_id}`.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `name` - The resource name of the Folder. Its format is `folders/{folder_id}`.
- `lifecycle_state` - The lifecycle state of the folder such as `ACTIVE` or `DELETE_REQUESTED`.

- `create_time` - Timestamp when the Folder was created. Assigned by the server. A timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds. Example: "2014-10-02T15:01:23.045123456Z".

## » Import

Folders can be imported using the folder autogenerated `name`, e.g.

```
# Both syntaxes are valid
$ terraform import google_folder.department1 1234567
$ terraform import google_folder.department1 folders/1234567
```

## » google\_folder\_iam\_binding

Allows creation and management of a single binding within IAM policy for an existing Google Cloud Platform folder.

**Note:** This resource *must not* be used in conjunction with `google_folder_iam_policy` or they will fight over what your policy should be.

**Note:** On create, this resource will overwrite members of any existing roles. Use `terraform import` and inspect the `terraform plan` output to ensure your existing members are preserved.

## » Example Usage

```
resource "google_folder" "department1" {
  display_name = "Department 1"
  parent      = "organizations/1234567"
}

resource "google_folder_iam_binding" "admin" {
  folder = "${google_folder.department1.name}"
  role   = "roles/editor"

  members = [
    "user:alice@gmail.com",
  ]
}
```

## » Argument Reference

The following arguments are supported:

- **folder** - (Required) The resource name of the folder the policy is attached to. Its format is `folders/{folder_id}`.
- **members** (Required) - An array of identities that will be granted the privilege in the **role**. Each entry can have one of the following values:
  - **user:{emailid}**: An email address that is associated with a specific Google account. For example, `alice@gmail.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
  - For more details on format and restrictions see <https://cloud.google.com/billing/reference/rest/v1/Policy#Binding>
- **role** - (Required) The role that should be applied. Only one `google_folder_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the folder's IAM policy.

## » Import

IAM binding imports use space-delimited identifiers; first the resource in question and then the role. These bindings can be imported using the **folder** and **role**, e.g.

```
$ terraform import google_folder_iam_binding.viewer "folder-name roles/viewer"
```

## » google\_\_folder\_\_iam\_\_member

Allows creation and management of a single member for a single binding within the IAM policy for an existing Google Cloud Platform folder.

**Note:** This resource *must not* be used in conjunction with `google_folder_iam_policy` or they will fight over what your policy should be. Similarly, roles con-

trolled by `google_folder_iam_binding` should not be assigned to using `google_folder_iam_member`.

## » Example Usage

```
resource "google_folder" "department1" {
  display_name = "Department 1"
  parent       = "organizations/1234567"
}

resource "google_folder_iam_member" "admin" {
  folder = "${google_folder.department1.name}"
  role   = "roles/editor"
  member = "user:alice@gmail.com"
}
```

## » Argument Reference

The following arguments are supported:

- **folder** - (Required) The resource name of the folder the policy is attached to. Its format is `folders/{folder_id}`.
- **member** - (Required) The identity that will be granted the privilege in the **role**. For more details on format and restrictions see <https://cloud.google.com/billing/reference/rest/v1/Policy#Binding> This field can have one of the following values:
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `etag` - (Computed) The etag of the folder's IAM policy.

## » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the `folder`, `role`, and member identity e.g.

```
$ terraform import google_folder_iam_member.my_project "folder-name roles/viewer user:foo@example.com"
```

## » `google__folder__iam__policy`

Allows creation and management of the IAM policy for an existing Google Cloud Platform folder.

## » Example Usage

```
resource "google_folder_iam_policy" "folder_admin_policy" {
  folder      = "${google_folder.department1.name}"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}

resource "google_folder" "department1" {
  display_name = "Department 1"
  parent       = "organizations/1234567"
}

data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}
```

## » Argument Reference

The following arguments are supported:

- **folder** - (Required) The resource name of the folder the policy is attached to. Its format is `folders/{folder_id}`.
- **policy\_data** - (Required) The `google_iam_policy` data source that represents the IAM policy that will be applied to the folder. This policy overrides any existing policy applied to the folder.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the folder's IAM policy. **etag** is used for optimistic concurrency control as a way to help prevent simultaneous updates of a policy from overwriting each other.

## » Import

A policy can be imported using the `folder`, e.g.

```
$ terraform import google_folder_iam_policy.my-folder-policy {{folder_id}}
```

## » `google__folder__organization__policy`

Allows management of Organization policies for a Google Folder. For more information see the official documentation and API.

## » Example Usage

To set policy with a boolean constraint:

```
resource "google_folder_organization_policy" "serial_port_policy" {
  folder      = "folders/123456789"
  constraint = "compute.disableSerialPortAccess"

  boolean_policy {
    enforced = true
  }
}
```

To set a policy with a list constraint:

```
resource "google_folder_organization_policy" "services_policy" {
  folder      = "folders/123456789"
  constraint = "serviceuser.services"

  list_policy {
    allow {
      all = true
    }
  }
}
```

Or to deny some services, use the following instead:

```
resource "google_folder_organization_policy" "services_policy" {
  folder      = "folders/123456789"
  constraint = "serviceuser.services"

  list_policy {
    suggested_values = "compute.googleapis.com"

    deny {
      values = ["cloudresourcemanager.googleapis.com"]
    }
  }
}
```

To restore the default folder organization policy, use the following instead:

```
resource "google_folder_organization_policy" "services_policy" {
  folder      = "folders/123456789"
  constraint = "serviceuser.services"

  restore_policy {
    default = true
  }
}
```

## » Argument Reference

The following arguments are supported:

- **folder** - (Required) The resource name of the folder to set the policy for. Its format is `folders/{folder_id}`.
- **constraint** - (Required) The name of the Constraint the Policy is configuring, for example, `serviceuser.services`. Check out the complete list



of available constraints.

- 
- **version** - (Optional) Version of the Policy. Default version is 0.
  - **boolean\_policy** - (Optional) A boolean policy is a constraint that is either enforced or not. Structure is documented below.
  - **list\_policy** - (Optional) A policy that can define specific values that are allowed or denied for the given constraint. It can also be used to allow or deny all values. Structure is documented below.
  - **restore\_policy** - (Optional) A restore policy is a constraint to restore the default policy. Structure is documented below.
- 

The **boolean\_policy** block supports:

- **enforced** - (Required) If true, then the Policy is enforced. If false, then any configuration is acceptable.

The **list\_policy** block supports:

- **allow** or **deny** - (Optional) One or the other must be set.
- **suggested\_values** - (Optional) The Google Cloud Console will try to default to a configuration that matches the value specified in this field.
- **inherit\_from\_parent** - (Optional) If set to true, the values from the effective Policy of the parent resource are inherited, meaning the values set in this Policy are added to the values inherited up the hierarchy.

The **allow** or **deny** blocks support:

- **all** - (Optional) The policy allows or denies all values.
- **values** - (Optional) The policy can define specific values that are allowed or denied.

The **restore\_policy** block supports:

- **default** - (Required) May only be set to true. If set, then the default Policy is restored.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the organization policy. **etag** is used for optimistic concurrency control as a way to help prevent simultaneous updates of a policy from overwriting each other.

- `update_time` - (Computed) The timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds, representing when the variable was last updated. Example: "2016-10-09T12:33:37.578138407Z".

## » `google_organization_policy`

Allows management of Organization policies for a Google Organization. For more information see the official documentation and API.

### » Example Usage

To set policy with a boolean constraint:

```
resource "google_organization_policy" "serial_port_policy" {
  org_id      = "123456789"
  constraint = "compute.disableSerialPortAccess"

  boolean_policy {
    enforced = true
  }
}
```

To set a policy with a list constraint:

```
resource "google_organization_policy" "services_policy" {
  org_id      = "123456789"
  constraint = "serviceuser.services"

  list_policy {
    allow {
      all = true
    }
  }
}
```

Or to deny some services, use the following instead:

```
resource "google_organization_policy" "services_policy" {
  org_id      = "123456789"
  constraint = "serviceuser.services"

  list_policy {
    suggested_values = "compute.googleapis.com"

    deny {
      values = ["cloudresourcemanager.googleapis.com"]
    }
  }
}
```

```
    }
  }
}
```

To restore the default organization policy, use the following instead:

```
resource "google_organization_policy" "services_policy" {
  org_id    = "123456789"
  constraint = "serviceuser.services"

  restore_policy {
    default = true
  }
}
```

## » Argument Reference

The following arguments are supported:

- **org\_id** - (Required) The numeric ID of the organization to set the policy for.
  - **constraint** - (Required) The name of the Constraint the Policy is configuring, for example, `serviceuser.services`. Check out the complete list of available constraints.
- 
- **version** - (Optional) Version of the Policy. Default version is 0.
  - **boolean\_policy** - (Optional) A boolean policy is a constraint that is either enforced or not. Structure is documented below.
  - **list\_policy** - (Optional) A policy that can define specific values that are allowed or denied for the given constraint. It can also be used to allow or deny all values. Structure is documented below.
  - **restore\_policy** - (Optional) A restore policy is a constraint to restore the default policy. Structure is documented below.
- 

The `boolean_policy` block supports:

- **enforced** - (Required) If true, then the Policy is enforced. If false, then any configuration is acceptable.

The `list_policy` block supports:

- **allow** or **deny** - (Optional) One or the other must be set.

- **suggested\_values** - (Optional) The Google Cloud Console will try to default to a configuration that matches the value specified in this field.
- **inherit\_from\_parent** - (Optional) If set to true, the values from the effective Policy of the parent resource are inherited, meaning the values set in this Policy are added to the values inherited up the hierarchy.

The **allow** or **deny** blocks support:

- **all** - (Optional) The policy allows or denies all values.
- **values** - (Optional) The policy can define specific values that are allowed or denied.

The **restore\_policy** block supports:

- **default** - (Required) May only be set to true. If set, then the default Policy is restored.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the organization policy. **etag** is used for optimistic concurrency control as a way to help prevent simultaneous updates of a policy from overwriting each other.
- **update\_time** - (Computed) The timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds, representing when the variable was last updated. Example: "2016-10-09T12:33:37.578138407Z".

## » Import

Organization Policies can be imported using the **org\_id** and the **constraint**, e.g.

```
$ terraform import google_organization_policy.services_policy 123456789:constraints/services_policy
```

## » google\_organization\_iam\_binding

Allows creation and management of a single binding within IAM policy for an existing Google Cloud Platform Organization.

**Note:** This resource **must not** be used in conjunction with **google\_organization\_iam\_member** for the **same role** or they will fight over what your policy should be.

**Note:** On create, this resource will overwrite members of any existing roles. Use `terraform import` and inspect the `terraform plan` output to ensure your existing members are preserved.

## » Example Usage

```
resource "google_organization_iam_binding" "binding" {
  org_id = "123456789"
  role    = "roles/browser"

  members = [
    "user:alice@gmail.com",
  ]
}
```

## » Argument Reference

The following arguments are supported:

- `org_id` - (Required) The numeric ID of the organization in which you want to create a custom role.
- `role` - (Required) The role that should be applied. Only one `google_organization_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- `members` - (Required) A list of users that the role should apply to. For more details on format and restrictions see <https://cloud.google.com/billing/reference/rest/v1/Policy#Binding>

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `etag` - (Computed) The etag of the organization's IAM policy.

## » Import

IAM binding imports use space-delimited identifiers; first the resource in question and then the role. These bindings can be imported using the `org_id` and role, e.g.

```
$ terraform import google_organization_iam_binding.my_org "your-org-id roles/viewer"
```

## » google\_organization\_iam\_custom\_role

Allows management of a customized Cloud IAM organization role. For more information see the official documentation and API.

**Warning:** Note that custom roles in GCP have the concept of a soft-delete. There are two issues that may arise from this and how roles are propagated. 1) creating a role may involve undeleting and then updating a role with the same name, possibly causing confusing behavior between undelete and update. 2) A deleted role is permanently deleted after 7 days, but it can take up to 30 more days (i.e. between 7 and 37 days after deletion) before the role name is made available again. This means a deleted role that has been deleted for more than 7 days cannot be changed at all by Terraform, and new roles cannot share that name.

### » Example Usage

This snippet creates a customized IAM organization role.

```
resource "google_organization_iam_custom_role" "my-custom-role" {
  role_id      = "myCustomRole"
  org_id       = "123456789"
  title        = "My Custom Role"
  description   = "A description"
  permissions  = ["iam.roles.list", "iam.roles.create", "iam.roles.delete"]
}
```

### » Argument Reference

The following arguments are supported:

- **role\_id** - (Required) The role id to use for this role.
- **org\_id** - (Required) The numeric ID of the organization in which you want to create a custom role.
- **title** - (Required) A human-readable title for the role.
- **permissions** (Required) The names of the permissions this role grants when bound in an IAM policy. At least one permission must be specified.
- **stage** - (Optional) The current launch stage of the role. Defaults to **GA**. List of possible stages is [here](#).
- **description** - (Optional) A human-readable description for the role.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `deleted` - (Optional) The current deleted state of the role.

## » Import

Customized IAM organization role can be imported using their URI, e.g.

```
$ terraform import google_organization_iam_custom_role.my-custom-role organizations/12345678
```

## » `google_organization_iam_member`

Allows creation and management of a single member for a single binding within the IAM policy for an existing Google Cloud Platform Organization.

**Note:** This resource **must not** be used in conjunction with `google_organization_iam_binding` for the **same role** or they will fight over what your policy should be.

## » Example Usage

```
resource "google_organization_iam_member" "binding" {
  org_id = "0123456789"
  role   = "roles/editor"
  member = "user:alice@gmail.com"
}
```

## » Argument Reference

The following arguments are supported:

- `org_id` - (Required) The numeric ID of the organization in which you want to create a custom role.
- `role` - (Required) The role that should be applied. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- `member` - (Required) The user that the role should apply to. For more details on format and restrictions see <https://cloud.google.com/billing/reference/rest/v1/Policy#Binding>

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `etag` - (Computed) The etag of the organization's IAM policy.

## » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the `org_id`, `role`, and member identity, e.g.

```
$ terraform import google_organization_iam_member.my_org "your-org-id roles/viewer user:foo@bar.com"
```

## » `google_organization_iam_policy`

Allows management of the entire IAM policy for an existing Google Cloud Platform Organization.

**Warning:** New organizations have several default policies which will, without extreme caution, be **overwritten** by use of this resource. The safest alternative is to use multiple `google_organization_iam_binding` resources. It is easy to use this resource to remove your own access to an organization, which will require a call to Google Support to have fixed, and can take multiple days to resolve. If you do use this resource, the best way to be sure that you are not making dangerous changes is to start by importing your existing policy, and examining the diff very closely.

**Note:** This resource **must not** be used in conjunction with `google_organization_iam_member` or `google_organization_iam_binding` or they will fight over what your policy should be.

## » Example Usage

```
resource "google_organization_iam_policy" "policy" {
  org_id = "123456789"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}

data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"
```



```

    members = [
        "user:jane@example.com",
    ]
}
}

```

## » Argument Reference

The following arguments are supported:

- **org\_id** - (Required) The numeric ID of the organization in which you want to create a custom role.
- **policy\_data** - (Required) The `google_iam_policy` data source that represents the IAM policy that will be applied to the organization. This policy overrides any existing policy applied to the organization.

## » Import

```
$ terraform import google_organization_iam_policy.my_org your-org-id
```

## » google\_\_project

Allows creation and management of a Google Cloud Platform project.

Projects created with this resource must be associated with an Organization. See the Organization documentation for more details.

The service account used to run Terraform when creating a `google_project` resource must have `roles/resourcemanager.projectCreator`. See the Access Control for Organizations Using IAM doc for more information.

Note that prior to 0.8.5, `google_project` functioned like a data source, meaning any project referenced by it had to be created and managed outside Terraform. As of 0.8.5, `google_project` functions like any other Terraform resource, with Terraform creating and managing the project. To replicate the old behavior, either:

- Use the project ID directly in whatever is referencing the project, using the `google_project_iam_policy` to replace the old `policy_data` property.
- Use the import functionality to import your pre-existing project into Terraform, where it can be referenced and used just like always, keeping in mind that Terraform will attempt to undo any changes made outside Terraform.

It's important to note that any project resources that were added to your Terraform config prior to 0.8.5 will continue to function as they always have, and will not be managed by Terraform. Only newly added projects are affected.

## » Example Usage

```
resource "google_project" "my_project" {
  name = "My Project"
  project_id = "your-project-id"
  org_id    = "1234567"
}
```

To create a project under a specific folder

```
resource "google_project" "my_project-in-a-folder" {
  name = "My Project"
  project_id = "your-project-id"
  folder_id = "${google_folder.department1.name}"
}
```

```
resource "google_folder" "department1" {
  display_name = "Department 1"
  parent       = "organizations/1234567"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The display name of the project.
- **project\_id** - (Required) The project ID. Changing this forces a new project to be created.
- **org\_id** - (Optional) The numeric ID of the organization this project belongs to. Changing this forces a new project to be created. Only one of **org\_id** or **folder\_id** may be specified. If the **org\_id** is specified then the project is created at the top level. Changing this forces the project to be migrated to the newly specified organization.
- **folder\_id** - (Optional) The numeric ID of the folder this project should be created under. Only one of **org\_id** or **folder\_id** may be specified. If the **folder\_id** is specified, then the project is created under the specified folder. Changing this forces the project to be migrated to the newly specified folder.

- **billing\_account** - (Optional) The alphanumeric ID of the billing account this project belongs to. The user or service account performing this operation with Terraform must have Billing Account Administrator privileges (**roles/billing.admin**) in the organization. See Google Cloud Billing API Access Control for more details.
- **skip\_delete** - (Optional) If true, the Terraform resource can be deleted without deleting the Project via the Google API.
- **labels** - (Optional) A set of key/value label pairs to assign to the project.
- **auto\_create\_network** - (Optional) Create the 'default' network automatically. Default **true**. If set to **false**, the default network will be deleted. Note that, for quota purposes, you will still need to have 1 network slot available to create the project successfully, even if you set **auto\_create\_network** to **false**, since the network will exist momentarily.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **number** - The numeric identifier of the project.

## » Import

Projects can be imported using the **project\_id**, e.g.

```
$ terraform import google_project.my_project your-project-id
```

## » IAM policy for projects

Three different resources help you manage your IAM policy for a project. Each of these resources serves a different use case:

- **google\_project\_iam\_policy**: Authoritative. Sets the IAM policy for the project and replaces any existing policy already attached.
- **google\_project\_iam\_binding**: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the project are preserved.
- **google\_project\_iam\_member**: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the project are preserved.

**Note:** `google_project_iam_policy` **cannot** be used in conjunction with `google_project_iam_binding` and `google_project_iam_member` or they will fight over what your policy should be.

**Note:** `google_project_iam_binding` resources **can be** used in conjunction with `google_project_iam_member` resources **only if** they do not grant privilege to the same role.

## » `google_project_iam_policy`

**Be careful!** You can accidentally lock yourself out of your project using this resource. Deleting a `google_project_iam_policy` removes access from anyone without organization-level access to the project. Proceed with caution. It's not recommended to use `google_project_iam_policy` with your provider project to avoid locking yourself out, and it should generally only be used with projects fully managed by Terraform.

```
resource "google_project_iam_policy" "project" {
  project      = "your-project-id"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}

data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}
```

## » `google_project_iam_binding`

**Note:** If `role` is set to `roles/owner` and you don't specify a user or service account you have access to in `members`, you can lock yourself out of your project.

```
resource "google_project_iam_binding" "project" {
  project = "your-project-id"
  role    = "roles/editor"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_project\_iam\_member

```
resource "google_project_iam_member" "project" {  
  project = "your-project-id"  
  role    = "roles/editor"  
  member  = "user:jane@example.com"  
}
```

## » Argument Reference

The following arguments are supported:

- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_project_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_project_iam_policy`) The `google_iam_policy` data source that represents the IAM policy that will be applied to the project. The policy will be merged with any existing policy applied to the project.

Changing this updates the policy.

Deleting this removes all policies from the project, locking out users without organization-level access.

- **project** - (Optional) The project ID. If not specified for `google_project_iam_binding` or `google_project_iam_member`, uses the ID of the project configured with the provider. Required for `google_project_iam_policy` - you must explicitly set the project, and it will not be inferred from the provider.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `etag` - (Computed) The etag of the project's IAM policy.

## » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the `project_id`, role, and member e.g.

```
$ terraform import google_project_iam_member.my_project "your-project-id roles/viewer user:u
```

IAM binding imports use space-delimited identifiers; the resource in question and the role. This binding resource can be imported using the `project_id` and role, e.g.

```
terraform import google_project_iam_binding.my_project "your-project-id roles/viewer"
```

IAM policy imports use the identifier of the resource in question. This policy resource can be imported using the `project_id`.

```
$ terraform import google_project_iam_policy.my_project your-project-id
```

## » IAM policy for projects

Three different resources help you manage your IAM policy for a project. Each of these resources serves a different use case:

- `google_project_iam_policy`: Authoritative. Sets the IAM policy for the project and replaces any existing policy already attached.
- `google_project_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the project are preserved.
- `google_project_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the project are preserved.

**Note:** `google_project_iam_policy` **cannot** be used in conjunction with `google_project_iam_binding` and `google_project_iam_member` or they will fight over what your policy should be.

**Note:** `google_project_iam_binding` resources **can be** used in conjunction with `google_project_iam_member` resources **only if** they do not grant privilege to the same role.

## » google\_project\_iam\_policy

**Be careful!** You can accidentally lock yourself out of your project using this resource. Deleting a `google_project_iam_policy` removes access from anyone without organization-level access to the project. Proceed with caution. It's not recommended to use `google_project_iam_policy` with your provider project to avoid locking yourself out, and it should generally only be used with projects fully managed by Terraform.

```
resource "google_project_iam_policy" "project" {
  project      = "your-project-id"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}

data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}
```

## » google\_project\_iam\_binding

**Note:** If `role` is set to `roles/owner` and you don't specify a user or service account you have access to in `members`, you can lock yourself out of your project.

```
resource "google_project_iam_binding" "project" {
  project = "your-project-id"
  role    = "roles/editor"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_project\_iam\_member

```
resource "google_project_iam_member" "project" {
  project = "your-project-id"
  role    = "roles/editor"
  member  = "user:jane@example.com"
}
```

## » Argument Reference

The following arguments are supported:

- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **user:{emailid}**: An email address that represents a specific Google account. For example, alice@gmail.com or joe@example.com.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_project_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_project_iam_policy`) The `google_iam_policy` data source that represents the IAM policy that will be applied to the project. The policy will be merged with any existing policy applied to the project.

Changing this updates the policy.

Deleting this removes all policies from the project, locking out users without organization-level access.

- **project** - (Optional) The project ID. If not specified for `google_project_iam_binding` or `google_project_iam_member`, uses the ID of the project configured with the provider. Required for `google_project_iam_policy` - you must explicitly set the project, and it will not be inferred from the provider.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the project's IAM policy.

## » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the



project\_id, role, and member e.g.

```
$ terraform import google_project_iam_member.my_project "your-project-id roles/viewer user:u
```

IAM binding imports use space-delimited identifiers; the resource in question and the role. This binding resource can be imported using the `project_id` and role, e.g.

```
terraform import google_project_iam_binding.my_project "your-project-id roles/viewer"
```

IAM policy imports use the identifier of the resource in question. This policy resource can be imported using the `project_id`.

```
$ terraform import google_project_iam_policy.my_project your-project-id
```

## » IAM policy for projects

Three different resources help you manage your IAM policy for a project. Each of these resources serves a different use case:

- `google_project_iam_policy`: Authoritative. Sets the IAM policy for the project and replaces any existing policy already attached.
- `google_project_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the project are preserved.
- `google_project_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the project are preserved.

**Note:** `google_project_iam_policy` **cannot** be used in conjunction with `google_project_iam_binding` and `google_project_iam_member` or they will fight over what your policy should be.

**Note:** `google_project_iam_binding` resources **can be** used in conjunction with `google_project_iam_member` resources **only if** they do not grant privilege to the same role.

## » `google_project_iam_policy`

**Be careful!** You can accidentally lock yourself out of your project using this resource. Deleting a `google_project_iam_policy` removes access from anyone without organization-level access to the project. Proceed with caution. It's not recommended to use `google_project_iam_policy` with your provider project to avoid locking yourself out, and it should generally only be used with projects fully managed by Terraform.

```
resource "google_project_iam_policy" "project" {  
  project      = "your-project-id"
```

```

    policy_data = "${data.google_iam_policy.admin.policy_data}"
  }

  data "google_iam_policy" "admin" {
    binding {
      role = "roles/editor"

      members = [
        "user:jane@example.com",
      ]
    }
  }
}

```

## » google\_project\_iam\_binding

**Note:** If role is set to `roles/owner` and you don't specify a user or service account you have access to in `members`, you can lock yourself out of your project.

```

resource "google_project_iam_binding" "project" {
  project = "your-project-id"
  role    = "roles/editor"

  members = [
    "user:jane@example.com",
  ]
}

```

## » google\_project\_iam\_member

```

resource "google_project_iam_member" "project" {
  project = "your-project-id"
  role    = "roles/editor"
  member  = "user:jane@example.com"
}

```

## » Argument Reference

The following arguments are supported:

- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.

- **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_project_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
  - **policy\_data** - (Required only by `google_project_iam_policy`) The `google_iam_policy` data source that represents the IAM policy that will be applied to the project. The policy will be merged with any existing policy applied to the project.
- Changing this updates the policy.
- Deleting this removes all policies from the project, locking out users without organization-level access.
- **project** - (Optional) The project ID. If not specified for `google_project_iam_binding` or `google_project_iam_member`, uses the ID of the project configured with the provider. Required for `google_project_iam_policy` - you must explicitly set the project, and it will not be inferred from the provider.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the project's IAM policy.

## » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the `project_id`, `role`, and `member` e.g.

```
$ terraform import google_project_iam_member.my_project "your-project-id roles/viewer user:u
```

IAM binding imports use space-delimited identifiers; the resource in question and the role. This binding resource can be imported using the `project_id` and `role`, e.g.

```
terraform import google_project_iam_binding.my_project "your-project-id roles/viewer"
```

IAM policy imports use the identifier of the resource in question. This policy resource can be imported using the `project_id`.

```
$ terraform import google_project_iam_policy.my_project your-project-id
```

## » `google_project_iam_custom_role`

Allows management of a customized Cloud IAM project role. For more information see the official documentation and API.

**Warning:** Note that custom roles in GCP have the concept of a soft-delete. There are two issues that may arise from this and how roles are propagated. 1) creating a role may involve undeleting and then updating a role with the same name, possibly causing confusing behavior between undelete and update. 2) A deleted role is permanently deleted after 7 days, but it can take up to 30 more days (i.e. between 7 and 37 days after deletion) before the role name is made available again. This means a deleted role that has been deleted for more than 7 days cannot be changed at all by Terraform, and new roles cannot share that name.

## » Example Usage

This snippet creates a customized IAM role.

```
resource "google_project_iam_custom_role" "my-custom-role" {
  role_id      = "myCustomRole"
  title        = "My Custom Role"
  description  = "A description"
  permissions  = ["iam.roles.list", "iam.roles.create", "iam.roles.delete"]
}
```

## » Argument Reference

The following arguments are supported:

- `role_id` - (Required) The role id to use for this role.
- `title` - (Required) A human-readable title for the role.
- `permissions` (Required) The names of the permissions this role grants when bound in an IAM policy. At least one permission must be specified.
- `project` - (Optional) The project that the service account will be created in. Defaults to the provider project configuration.

- **stage** - (Optional) The current launch stage of the role. Defaults to **GA**. List of possible stages is [here](#).
- **description** - (Optional) A human-readable description for the role.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **deleted** - (Optional) The current deleted state of the role.

## » Import

Customized IAM project role can be imported using their URI, e.g.

```
$ terraform import google_project_iam_custom_role.my-custom-role projects/my-project/roles/my-custom-role
```

## » google\_project\_organization\_policy

Allows management of Organization policies for a Google Project. For more information see the official documentation and API.

## » Example Usage

To set policy with a boolean constraint:

```
resource "google_project_organization_policy" "serial_port_policy" {
  project      = "your-project-id"
  constraint   = "compute.disableSerialPortAccess"

  boolean_policy {
    enforced = true
  }
}
```

To set a policy with a list constraint:

```
resource "google_project_organization_policy" "services_policy" {
  project      = "your-project-id"
  constraint   = "serviceuser.services"

  list_policy {
    allow {
```

```

        all = true
    }
}
}

```

Or to deny some services, use the following instead:

```

resource "google_project_organization_policy" "services_policy" {
  project      = "your-project-id"
  constraint    = "serviceuser.services"

  list_policy {
    suggested_values = "compute.googleapis.com"

    deny {
      values = ["cloudresourcemanager.googleapis.com"]
    }
  }
}

```

To restore the default project organization policy, use the following instead:

```

resource "google_project_organization_policy" "services_policy" {
  project      = "your-project-id"
  constraint    = "serviceuser.services"

  restore_policy {
    default = true
  }
}

```

## » Argument Reference

The following arguments are supported:

- **project** - (Required) The project id of the project to set the policy for.
  - **constraint** - (Required) The name of the Constraint the Policy is configuring, for example, `serviceuser.services`. Check out the complete list of available constraints.
- 
- **version** - (Optional) Version of the Policy. Default version is 0.
  - **boolean\_policy** - (Optional) A boolean policy is a constraint that is either enforced or not. Structure is documented below.

- **list\_policy** - (Optional) A policy that can define specific values that are allowed or denied for the given constraint. It can also be used to allow or deny all values. Structure is documented below.
- **restore\_policy** - (Optional) A restore policy is a constraint to restore the default policy. Structure is documented below.

---

The **boolean\_policy** block supports:

- **enforced** - (Required) If true, then the Policy is enforced. If false, then any configuration is acceptable.

The **list\_policy** block supports:

- **allow** or **deny** - (Optional) One or the other must be set.
- **suggested\_values** - (Optional) The Google Cloud Console will try to default to a configuration that matches the value specified in this field.
- **inherit\_from\_parent** - (Optional) If set to true, the values from the effective Policy of the parent resource are inherited, meaning the values set in this Policy are added to the values inherited up the hierarchy.

The **allow** or **deny** blocks support:

- **all** - (Optional) The policy allows or denies all values.
- **values** - (Optional) The policy can define specific values that are allowed or denied.

The **restore\_policy** block supports:

- **default** - (Required) May only be set to true. If set, then the default Policy is restored.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the organization policy. **etag** is used for optimistic concurrency control as a way to help prevent simultaneous updates of a policy from overwriting each other.
- **update\_time** - (Computed) The timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds, representing when the variable was last updated. Example: "2016-10-09T12:33:37.578138407Z".

## » `google__project__service`

Allows management of a single API service for an existing Google Cloud Platform project.

For a list of services available, visit the [API library page](#) or run `gcloud services list`.

**Note:** This resource *must not* be used in conjunction with `google_project_services` or they will fight over which services should be enabled.

## » Example Usage

```
resource "google_project_service" "project" {
  project = "your-project-id"
  service = "iam.googleapis.com"

  disable_dependent_services = true
}
```

## » Argument Reference

The following arguments are supported:

- `service` - (Required) The service to enable.
- `project` - (Optional) The project ID. If not provided, the provider project is used.
- `disable_dependent_services` - (Optional) If `true`, services that are enabled and which depend on this service should also be disabled when this service is destroyed. If `false` or unset, an error will be generated if any enabled services depend on this service when destroying it.
- `disable_on_destroy` - (Optional) If true, disable the service when the terraform resource is destroyed. Defaults to true. May be useful in the event that a project is long-lived but the infrastructure running in that project changes frequently.

## » Import

Project services can be imported using the `project_id` and `service`, e.g.

```
$ terraform import google_project_service.my_project your-project-id/iam.googleapis.com
```



## » google\_\_project\_\_services

Allows management of enabled API services for an existing Google Cloud Platform project. Services in an existing project that are not defined in the config will be removed.

For a list of services available, visit the API library page or run `gcloud services list`.

**Note:** This resource attempts to be the authoritative source on *all* enabled APIs, which often leads to conflicts when certain actions enable other APIs. If you do not need to ensure that *exclusively* a particular set of APIs are enabled, you should most likely use the `google_project_service` resource, one resource per API.

## » Example Usage

```
resource "google_project_services" "project" {
  project = "your-project-id"
  services = ["iam.googleapis.com", "cloudresourcemanager.googleapis.com"]
}
```

## » Argument Reference

The following arguments are supported:

- **project** - (Required) The project ID. Changing this forces Terraform to attempt to disable all previously managed API services in the previous project.
- **services** - (Required) The list of services that are enabled. Supports update.

## » Import

Project services can be imported using the `project_id`, e.g.

```
$ terraform import google_project_services.my_project your-project-id
```

## » google\_\_project\_\_usage\_\_export\_\_bucket

Sets up a usage export bucket for a particular project. A usage export bucket is a pre-configured GCS bucket which is set up to receive daily and monthly reports of the GCE resources used.

For more information see the Docs and for further details, the API Documentation.

**Note:** You should specify only one of these per project. If there are two or more they will fight over which bucket the reports should be stored in. It is safe to have multiple resources with the same backing bucket.

## » Example Usage

```
resource "google_project_usage_export_bucket" "usage_export" {
  project      = "development-project"
  bucket_name  = "usage-tracking-bucket"
}
```

## » Argument Reference

- `bucket_name`: (Required) The bucket to store reports in.
- 
- `prefix`: (Optional) A prefix for the reports, for instance, the project name.
  - `project`: (Optional) The project to set the export bucket on. If it is not provided, the provider project is used.

## » Import

A project's Usage Export Bucket can be imported using this format:

```
$ terraform import google_project_usage_export_bucket.usage_export {{project}}
```

## » google\_\_resource\_\_manager\_\_lien

A Lien represents an encumbrance on the actions that can be performed on a resource.

## » Example Usage - Resource Manager Lien

```
resource "google_resource_manager_lien" "lien" {
  parent = "projects/${google_project.project.number}"
  restrictions = ["resourcemanager.projects.delete"]
  origin = "machine-readable-explanation"
  reason = "This project is an important environment"
```

```

}

resource "google_project" "project" {
  project_id = "staging-project"
  name = "A very important project!"
}

```

## » Argument Reference

The following arguments are supported:

- **reason** - (Required) Concise user-visible strings indicating why an action cannot be performed on a resource. Maximum length of 200 characters.
- **origin** - (Required) A stable, user-visible/meaningful string identifying the origin of the Lien, intended to be inspected programmatically. Maximum length of 200 characters.
- **parent** - (Required) A reference to the resource this Lien is attached to. The server will validate the parent against those for which Liens are supported. Since a variety of objects can have Liens against them, you must provide the type prefix (e.g. "projects/my-project-name").
- **restrictions** - (Required) The types of operations which should be blocked as a result of this Lien. Each value should correspond to an IAM permission. The server will validate the permissions against those for which Liens are supported. An empty list is meaningless and will be rejected. e.g. ['resourceanalyzer.projects.delete']

---

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **name** - A system-generated unique identifier for this Lien.
- **create\_time** - Time of creation

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

Lien can be imported using any of these accepted formats:

```
$ terraform import google_resource_manager_lien.default {{parent}}/{{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_service\_\_account

Allows management of a Google Cloud Platform service account

Creation of service accounts is eventually consistent, and that can lead to errors when you try to apply ACLs to service accounts immediately after creation. If using these resources in the same config, you can add a `sleep` using `local-exec`.

## » Example Usage

This snippet creates a service account, then gives it objectViewer permission in a project.

```
resource "google_service_account" "object_viewer" {
  account_id   = "object-viewer"
  display_name = "Object viewer"
}
```

## » Argument Reference

The following arguments are supported:

- **account\_id** - (Required) The account id that is used to generate the service account email address and a stable unique id. It is unique within a project, must be 6-30 characters long, and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])` to comply with RFC1035. Changing this forces a new service account to be created.
- **display\_name** - (Optional) The display name for the service account. Can be updated without creating a new resource.
- **project** - (Optional) The ID of the project that the service account will be created in. Defaults to the provider project configuration.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **email** - The e-mail address of the service account. This value should be referenced from any `google_iam_policy` data sources that would grant the service account privileges.
- **name** - The fully-qualified name of the service account.
- **unique\_id** - The unique id of the service account.

## » Import

Service accounts can be imported using their URI, e.g.

```
$ terraform import google_service_account.my_sa projects/my-project/serviceAccounts/my-sa@my
```

## » IAM policy for service account

When managing IAM roles, you can treat a service account either as a resource or as an identity. This resource is to add iam policy bindings to a service account resource **to configure permissions for who can edit the service account**. To configure permissions for a service account to act as an identity that can manage other GCP resources, use the `google_project_iam` set of resources.

Three different resources help you manage your IAM policy for a service account. Each of these resources serves a different use case:

- **google\_service\_account\_iam\_policy**: Authoritative. Sets the IAM policy for the service account and replaces any existing policy already attached.
- **google\_service\_account\_iam\_binding**: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the service account are preserved.
- **google\_service\_account\_iam\_member**: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the service account are preserved.

**Note:** `google_service_account_iam_policy` **cannot** be used in conjunction with `google_service_account_iam_binding` and `google_service_account_iam_member` or they will fight over what your policy should be.

**Note:** `google_service_account_iam_binding` resources **can be** used in conjunction with `google_service_account_iam_member` resources **only if** they do not grant privilege to the same role.

## » google\_service\_account\_iam\_policy

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/iam.serviceAccountUser"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_service_account" "sa" {
  account_id = "my-service-account"
  display_name = "A service account that only Jane can interact with"
}

resource "google_service_account_iam_policy" "admin-account-iam" {
  service_account_id = "${google_service_account.sa.name}"
  policy_data         = "${data.google_iam_policy.admin.policy_data}"
}
```

## » google\_service\_account\_iam\_binding

```
resource "google_service_account" "sa" {
  account_id = "my-service-account"
  display_name = "A service account that only Jane can use"
}

resource "google_service_account_iam_binding" "admin-account-iam" {
  service_account_id = "${google_service_account.sa.name}"
  role                = "roles/iam.serviceAccountUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_service\_account\_iam\_member

```
data "google_compute_default_service_account" "default" { }
```

```
resource "google_service_account" "sa" {
  account_id = "my-service-account"
```

```

    display_name = "A service account that Jane can use"
  }

resource "google_service_account_iam_member" "admin-account-iam" {
  service_account_id = "${google_service_account.sa.name}"
  role               = "roles/iam.serviceAccountUser"
  member             = "user:jane@example.com"
}

# Allow SA service account use the default GCE account
resource "google_service_account_iam_member" "gce-default-account-iam" {
  service_account_id = "${data.google_compute_default_service_account.default.name}"
  role               = "roles/iam.serviceAccountUser"
  member             = "serviceAccount:${google_service_account.sa.email}"
}

```

## » Argument Reference

The following arguments are supported:

- **service\_account\_id** - (Required) The fully-qualified name of the service account to apply policy to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_service_account_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_service_account_iam_policy`) The policy data generated by a `google_iam_policy` data source.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `etag` - (Computed) The etag of the service account IAM policy.

## » Import

Service account IAM resources can be imported using the project, service account email, role and member identity.

```
$ terraform import google_service_account_iam_policy.admin-account-iam projects/{your-project-id}
```

```
$ terraform import google_service_account_iam_binding.admin-account-iam "projects/{your-project-id}/roles/{role-id}"
```

```
$ terraform import google_service_account_iam_member.admin-account-iam "projects/{your-project-id}/roles/{role-id}/members/{member-id}"
```

## » IAM policy for service account

When managing IAM roles, you can treat a service account either as a resource or as an identity. This resource is to add iam policy bindings to a service account resource **to configure permissions for who can edit the service account**. To configure permissions for a service account to act as an identity that can manage other GCP resources, use the `google_project_iam` set of resources.

Three different resources help you manage your IAM policy for a service account. Each of these resources serves a different use case:

- `google_service_account_iam_policy`: Authoritative. Sets the IAM policy for the service account and replaces any existing policy already attached.
- `google_service_account_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the service account are preserved.
- `google_service_account_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the service account are preserved.

**Note:** `google_service_account_iam_policy` **cannot** be used in conjunction with `google_service_account_iam_binding` and `google_service_account_iam_member` or they will fight over what your policy should be.

**Note:** `google_service_account_iam_binding` resources **can be** used in conjunction with `google_service_account_iam_member` resources **only if** they do not grant privilege to the same role.



## » google\_service\_account\_iam\_policy

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/iam.serviceAccountUser"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_service_account" "sa" {
  account_id   = "my-service-account"
  display_name = "A service account that only Jane can interact with"
}

resource "google_service_account_iam_policy" "admin-account-iam" {
  service_account_id = "${google_service_account.sa.name}"
  policy_data         = "${data.google_iam_policy.admin.policy_data}"
}
```

## » google\_service\_account\_iam\_binding

```
resource "google_service_account" "sa" {
  account_id   = "my-service-account"
  display_name = "A service account that only Jane can use"
}

resource "google_service_account_iam_binding" "admin-account-iam" {
  service_account_id = "${google_service_account.sa.name}"
  role                = "roles/iam.serviceAccountUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_service\_account\_iam\_member

```
data "google_compute_default_service_account" "default" { }
```

```
resource "google_service_account" "sa" {
  account_id   = "my-service-account"
```

```

    display_name = "A service account that Jane can use"
  }

resource "google_service_account_iam_member" "admin-account-iam" {
  service_account_id = "${google_service_account.sa.name}"
  role                = "roles/iam.serviceAccountUser"
  member              = "user:jane@example.com"
}

# Allow SA service account use the default GCE account
resource "google_service_account_iam_member" "gce-default-account-iam" {
  service_account_id = "${data.google_compute_default_service_account.default.name}"
  role                = "roles/iam.serviceAccountUser"
  member              = "serviceAccount:${google_service_account.sa.email}"
}

```

## » Argument Reference

The following arguments are supported:

- **service\_account\_id** - (Required) The fully-qualified name of the service account to apply policy to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_service_account_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_service_account_iam_policy`) The policy data generated by a `google_iam_policy` data source.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `etag` - (Computed) The etag of the service account IAM policy.

## » Import

Service account IAM resources can be imported using the project, service account email, role and member identity.

```
$ terraform import google_service_account_iam_policy.admin-account-iam projects/{your-project-id}
```

```
$ terraform import google_service_account_iam_binding.admin-account-iam "projects/{your-project-id}/roles/{role-id}"
```

```
$ terraform import google_service_account_iam_member.admin-account-iam "projects/{your-project-id}/roles/{role-id}/members/{member-id}"
```

## » IAM policy for service account

When managing IAM roles, you can treat a service account either as a resource or as an identity. This resource is to add iam policy bindings to a service account resource **to configure permissions for who can edit the service account**. To configure permissions for a service account to act as an identity that can manage other GCP resources, use the `google_project_iam` set of resources.

Three different resources help you manage your IAM policy for a service account. Each of these resources serves a different use case:

- `google_service_account_iam_policy`: Authoritative. Sets the IAM policy for the service account and replaces any existing policy already attached.
- `google_service_account_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the service account are preserved.
- `google_service_account_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the service account are preserved.

**Note:** `google_service_account_iam_policy` **cannot** be used in conjunction with `google_service_account_iam_binding` and `google_service_account_iam_member` or they will fight over what your policy should be.

**Note:** `google_service_account_iam_binding` resources **can be** used in conjunction with `google_service_account_iam_member` resources **only if** they do not grant privilege to the same role.

## » google\_service\_account\_iam\_policy

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/iam.serviceAccountUser"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_service_account" "sa" {
  account_id = "my-service-account"
  display_name = "A service account that only Jane can interact with"
}

resource "google_service_account_iam_policy" "admin-account-iam" {
  service_account_id = "${google_service_account.sa.name}"
  policy_data         = "${data.google_iam_policy.admin.policy_data}"
}
```

## » google\_service\_account\_iam\_binding

```
resource "google_service_account" "sa" {
  account_id = "my-service-account"
  display_name = "A service account that only Jane can use"
}

resource "google_service_account_iam_binding" "admin-account-iam" {
  service_account_id = "${google_service_account.sa.name}"
  role                = "roles/iam.serviceAccountUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_service\_account\_iam\_member

```
data "google_compute_default_service_account" "default" { }
```

```
resource "google_service_account" "sa" {
  account_id = "my-service-account"
```

```

    display_name = "A service account that Jane can use"
  }

  resource "google_service_account_iam_member" "admin-account-iam" {
    service_account_id = "${google_service_account.sa.name}"
    role               = "roles/iam.serviceAccountUser"
    member             = "user:jane@example.com"
  }

  # Allow SA service account use the default GCE account
  resource "google_service_account_iam_member" "gce-default-account-iam" {
    service_account_id = "${data.google_compute_default_service_account.default.name}"
    role               = "roles/iam.serviceAccountUser"
    member             = "serviceAccount:${google_service_account.sa.email}"
  }

```

## » Argument Reference

The following arguments are supported:

- **service\_account\_id** - (Required) The fully-qualified name of the service account to apply policy to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_service_account_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_service_account_iam_policy`) The policy data generated by a `google_iam_policy` data source.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `etag` - (Computed) The etag of the service account IAM policy.

## » Import

Service account IAM resources can be imported using the project, service account email, role and member identity.

```
$ terraform import google_service_account_iam_policy.admin-account-iam projects/{your-project-id}
```

```
$ terraform import google_service_account_iam_binding.admin-account-iam "projects/{your-project-id}/roles/{role-id}"
```

```
$ terraform import google_service_account_iam_member.admin-account-iam "projects/{your-project-id}/roles/{role-id}/members/{member-id}"
```

## » `google_service_account_key`

Creates and manages service account key-pairs, which allow the user to establish identity of a service account outside of GCP. For more information, see the [official documentation](#) and [API](#).

## » Example Usage, creating a new Key Pair

```
resource "google_service_account" "myaccount" {
  account_id = "myaccount"
  display_name = "My Service Account"
}

resource "google_service_account_key" "mykey" {
  service_account_id = "${google_service_account.myaccount.name}"
  public_key_type = "TYPE_X509_PEM_FILE"
}
```

## » Example Usage, save key in Kubernetes secret

```
resource "google_service_account" "myaccount" {
  account_id = "myaccount"
  display_name = "My Service Account"
}
```

```

resource "google_service_account_key" "mykey" {
  service_account_id = "${google_service_account.myaccount.name}"
}

resource "kubernetes_secret" "google-application-credentials" {
  metadata = {
    name = "google-application-credentials"
  }
  data {
    credentials.json = "${base64decode(google_service_account_key.mykey.private_key)}"
  }
}

```

## » Create new Key Pair, encrypting the private key with a PGP Key

```

resource "google_service_account" "myaccount" {
  account_id = "myaccount"
  display_name = "My Service Account"
}

resource "google_service_account_key" "mykey" {
  service_account_id = "${google_service_account.myaccount.name}"
  pgp_key = "keybase:keybaseusername"
  public_key_type = "TYPE_X509_PEM_FILE"
}

```

## » Argument Reference

The following arguments are supported:

- **service\_account\_id** - (Required) The Service account id of the Key Pair. This can be a string in the format `{ACCOUNT}` or `projects/{PROJECT_ID}/serviceAccounts/{ACCOUNT}`, where `{ACCOUNT}` is the email address or unique id of the service account. If the `{ACCOUNT}` syntax is used, the project will be inferred from the account.
- **key\_algorithm** - (Optional) The algorithm used to generate the key. `KEY_ALG_RSA_2048` is the default algorithm. Valid values are listed at `ServiceAccountPrivateKeyType` (only used on create)
- **public\_key\_type** (Optional) The output format of the public key requested. `X509_PEM` is the default output format.

- **private\_key\_type** (Optional) The output format of the private key. `TYPE_GOOGLE_CREDENTIALS_FILE` is the default output format.
- **pgp\_key** – (Optional) An optional PGP key to encrypt the resulting private key material. Only used when creating or importing a new key pair. May either be a base64-encoded public key or a `keybase:keybaseusername` string for looking up in Vault.

**NOTE:** a PGP key is not required, however it is strongly encouraged. Without a PGP key, the private key material will be stored in state unencrypted.

## » Attributes Reference

The following attributes are exported in addition to the arguments listed above:

- **name** - The name used for this key pair
- **public\_key** - The public key, base64 encoded
- **private\_key** - The private key in JSON format, base64 encoded. This is what you normally get as a file when creating service account keys through the CLI or web console. This is only populated when creating a new key, and when no **pgp\_key** is provided.
- **private\_key\_encrypted** – The private key material, base 64 encoded and encrypted with the given **pgp\_key**. This is only populated when creating a new key and **pgp\_key** is supplied
- **private\_key\_fingerprint** - The MD5 public key fingerprint for the encrypted private key. This is only populated when creating a new key and **pgp\_key** is supplied
- **valid\_after** - The key can be used after this timestamp. A timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds. Example: "2014-10-02T15:01:23.045123456Z".
- **valid\_before** - The key can be used before this timestamp. A timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds. Example: "2014-10-02T15:01:23.045123456Z".

## » google\_\_cloud\_\_scheduler\_\_job

A scheduled job that can publish a pubsub message or a http request every X interval of time, using crontab format string

To get more information about Job, see:

- API documentation
- How-to Guides





OPEN IN GOOGLE CLOUD SHELL

### » Example Usage - Scheduler Job Pubsub

```
resource "google_pubsub_topic" "topic" {
  name = "job-topic"
}

resource "google_cloud_scheduler_job" "job" {
  name      = "test-job"
  description = "test job"
  schedule = "*/2 * * * *"

  pubsub_target {
    topic_name = "${google_pubsub_topic.topic.id}"
    data = "${base64encode("test")}"
  }
}
```



OPEN IN GOOGLE CLOUD SHELL

### » Example Usage - Scheduler Job Http

```
resource "google_cloud_scheduler_job" "job" {
  name      = "test-job"
  description = "test http job"
  schedule = "*/8 * * * *"
  time_zone = "America/New_York"

  http_target {
    http_method = "POST"
    uri = "https://example.com/ping"
  }
}
```



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Scheduler Job App Engine

```
resource "google_cloud_scheduler_job" "job" {
  name      = "test-job"
  schedule  = "*/4 * * * *"
  description = "test app engine job"
  time_zone = "Europe/London"

  app_engine_http_target {
    http_method = "POST"

    app_engine_routing {
      service = "web"
      version = "prod"
      instance = "my-instance-001"
    }
  }

  relative_uri = "/ping"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the job.
  - **region** - (Required) Region where the scheduler job resides
- 
- **description** - (Optional) A human-readable description for the job. This string must not contain more than 500 characters.
  - **schedule** - (Optional) Describes the schedule on which the job will be executed.
  - **time\_zone** - (Optional) Specifies the time zone to be used in interpreting schedule. The value of this field must be a time zone name from the tz database.

- **retry\_config** - (Optional) By default, if a job does not complete successfully, meaning that an acknowledgement is not received from the handler, then it will be retried with exponential backoff according to the settings Structure is documented below.
- **pubsub\_target** - (Optional) Pub/Sub target If the job providers a Pub/Sub target the cron will publish a message to the provided topic Structure is documented below.
- **app\_engine\_http\_target** - (Optional) App Engine HTTP target. If the job providers a App Engine HTTP target the cron will send a request to the service instance Structure is documented below.
- **http\_target** - (Optional) HTTP target. If the job providers a http\_target the cron will send a request to the targeted url Structure is documented below.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **retry\_config** block supports:

- **retry\_count** - (Optional) The number of attempts that the system will make to run a job using the exponential backoff procedure described by maxDoublings. Values greater than 5 and negative values are not allowed.
- **max\_retry\_duration** - (Optional) The time limit for retrying a failed job, measured from time when an execution was first attempted. If specified with retryCount, the job will be retried until both limits are reached. A duration in seconds with up to nine fractional digits, terminated by 's'.
- **min\_backoff\_duration** - (Optional) The minimum amount of time to wait before retrying a job after it fails. A duration in seconds with up to nine fractional digits, terminated by 's'.
- **max\_backoff\_duration** - (Optional) The maximum amount of time to wait before retrying a job after it fails. A duration in seconds with up to nine fractional digits, terminated by 's'.
- **max\_doublings** - (Optional) The time between retries will double maxDoublings times. A job's retry interval starts at minBackoffDuration, then doubles maxDoublings times, then increases linearly, and finally retries retries at intervals of maxBackoffDuration up to retryCount times.

The **pubsub\_target** block supports:

- **topic\_name** - (Required) The name of the Cloud Pub/Sub topic to which messages will be published when a job is delivered. The topic name must be in the same format as required by PubSub's PublishRequest.name, for example projects/PROJECT\_ID/topics/TOPIC\_ID.

- **data** - (Optional) The message payload for PubsubMessage. Pubsub message must contain either non-empty data, or at least one attribute.
- **attributes** - (Optional) Attributes for PubsubMessage. Pubsub message must contain either non-empty data, or at least one attribute.

The `app_engine_http_target` block supports:

- **http\_method** - (Optional) Which HTTP method to use for the request.
- **app\_engine\_routing** - (Optional) App Engine Routing setting for the job. Structure is documented below.
- **relative\_uri** - (Required) The relative URI. The relative URL must begin with "/" and must be a valid HTTP relative URL. It can contain a path, query string arguments, and # fragments. If the relative URL is empty, then the root path "/" will be used. No spaces are allowed, and the maximum length allowed is 2083 characters
- **body** - (Optional) HTTP request body. A request body is allowed only if the HTTP method is POST or PUT. It will result in invalid argument error to set a body on a job with an incompatible HttpMethod.
- **headers** - (Optional) HTTP request headers. This map contains the header field names and values. Headers can be set when the job is created.

The `app_engine_routing` block supports:

- **service** - (Optional) App service. By default, the job is sent to the service which is the default service when the job is attempted.
- **version** - (Optional) App version. By default, the job is sent to the version which is the default version when the job is attempted.
- **instance** - (Optional) App instance. By default, the job is sent to an instance which is available when the job is attempted.

The `http_target` block supports:

- **uri** - (Required) The full URI path that the request will be sent to.
- **http\_method** - (Optional) Which HTTP method to use for the request.
- **body** - (Optional) HTTP request body. A request body is allowed only if the HTTP method is POST, PUT, or PATCH. It is an error to set body on a job with an incompatible HttpMethod.
- **headers** - (Optional) This map contains the header field names and values. Repeated headers are not supported, but a header value can contain commas.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Job can be imported using any of these accepted formats:

```
$ terraform import google_cloud_scheduler_job.default projects/{{project}}/locations/{{region}}/jobs/{{name}}
$ terraform import google_cloud_scheduler_job.default {{project}}/{{region}}/{{name}}
$ terraform import google_cloud_scheduler_job.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_address

Represents an Address resource.

Each virtual machine instance has an ephemeral internal IP address and, optionally, an external IP address. To communicate between instances on the same network, you can use an instance's internal IP address. To communicate with the Internet and instances outside of the same network, you must specify the instance's external IP address.

Internal IP addresses are ephemeral and only belong to an instance for the lifetime of the instance; if the instance is deleted and recreated, the instance is assigned a new internal IP address, either by Compute Engine or by you. External IP addresses can be either ephemeral or static.

To get more information about Address, see:

- API documentation
- How-to Guides
  - Reserving a Static External IP Address
  - Reserving a Static Internal IP Address



OPEN IN GOOGLE CLOUD SHELL

### » Example Usage - Address Basic

```
resource "google_compute_address" "ip_address" {  
  name = "my-address"  
}
```



OPEN IN GOOGLE CLOUD SHELL

### » Example Usage - Address With Subnetwork

```
resource "google_compute_network" "default" {  
  name = "my-network"  
}  
  
resource "google_compute_subnetwork" "default" {  
  name           = "my-subnet"  
  ip_cidr_range = "10.0.0.0/16"  
  region        = "us-central1"  
  network       = "${google_compute_network.default.self_link}"  
}  
  
resource "google_compute_address" "internal_with_subnet_and_address" {  
  name           = "my-internal-address"  
  subnetwork     = "${google_compute_subnetwork.default.self_link}"  
  address_type   = "INTERNAL"  
  address        = "10.0.42.42"  
  region        = "us-central1"  
}
```



OPEN IN GOOGLE CLOUD SHELL

### » Example Usage - Instance With Ip

```
resource "google_compute_address" "static" {  
  name = "ipv4-address"  
}
```

```

data "google_compute_image" "debian_image" {
  family = "debian-9"
  project = "debian-cloud"
}

resource "google_compute_instance" "instance_with_ip" {
  name          = "vm-instance"
  machine_type  = "f1-micro"
  zone          = "us-central1-a"

  boot_disk {
    initialize_params{
      image = "${data.google_compute_image.debian_image.self_link}"
    }
  }

  network_interface {
    network = "default"
    access_config {
      nat_ip = "${google_compute_address.static.address}"
    }
  }
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- **address** - (Optional) The static external IP address represented by this resource. Only IPv4 is supported. An address may only be specified for INTERNAL address types. The IP address must be inside the specified subnetwork, if any.
- **address\_type** - (Optional) The type of address to reserve, either INTERNAL or EXTERNAL. If unspecified, defaults to EXTERNAL.
- **description** - (Optional) An optional description of this resource.

- **network\_tier** - (Optional) The networking tier used for configuring this address. This field can take the following values: PREMIUM or STANDARD. If this field is not specified, it is assumed to be PREMIUM.
- **subnetwork** - (Optional) The URL of the subnetwork in which to reserve the address. If an IP address is specified, it must be within the subnetwork's IP range. This field can only be used with INTERNAL type with GCE\_ENDPOINT/DNS\_RESOLVER purposes.
- **labels** - (Optional, Beta) Labels to apply to this address. A list of key->value pairs.
- **region** - (Optional) The Region in which the created address should reside. If it is not provided, the provider region is used.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **users** - The URLs of the resources that are using this address.
- **label\_fingerprint** - The fingerprint used for optimistic locking of this resource. Used internally during updates.
- **self\_link** - The URI of the created resource.
- **address** - The IP of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

Address can be imported using any of these accepted formats:

```
$ terraform import google_compute_address.default projects/{{project}}/regions/{{region}}/ad
$ terraform import google_compute_address.default {{project}}/{{region}}/{{name}}
$ terraform import google_compute_address.default {{name}}
```



If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_compute_attached_disk`

Persistent disks can be attached to a compute instance using the `attached_disk` section within the compute instance configuration. However there may be situations where managing the attached disks via the compute instance config isn't preferable or possible, such as attaching dynamic numbers of disks using the `count` variable.

To get more information about attaching disks, see:

- API documentation
- Resource: `google_compute_disk`
- How-to Guides
  - Adding a persistent disk

## » Example Usage

```
resource "google_compute_attached_disk" "default" {  
  disk = "${google_compute_disk.default.self_link}"  
  instance = "${google_compute_instance.default.self_link}"  
}
```

## » Argument Reference

The following arguments are supported:

- `instance` - (Required) `name` or `self_link` of the compute instance that the disk will be attached to. If the `self_link` is provided then `zone` and `project` are extracted from the self link. If only the name is used then `zone` and `project` must be defined as properties on the resource or provider.
  - `disk` - (Required) `name` or `self_link` of the disk that will be attached.
- 
- `project` - (Optional) The project that the referenced compute instance is a part of. If `instance` is referenced by its `self_link` the project defined in the link will take precedence.

- **zone** - (Optional) The zone that the referenced compute instance is located within. If **instance** is referenced by its **self\_link** the zone defined in the link will take precedence.
- **device\_name** - (Optional) Specifies a unique device name of your choice that is reflected into the `/dev/disk/by-id/google-*` tree of a Linux operating system running within the instance. This name can be used to reference the device for mounting, resizing, and so on, from within the instance.

If not specified, the server chooses a default device name to apply to this disk, in the form `persistent-disks-x`, where `x` is a number assigned by Google Compute Engine.

- **mode** - (Optional) The mode in which to attach this disk, either `READ_WRITE` or `READ_ONLY`. If not specified, the default is to attach the disk in `READ_WRITE` mode.

Possible values: `"READ_ONLY"` `"READ_WRITE"`

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 5 minutes.
- **delete** - Default is 5 minutes.

## » Import

Attached Disk can be imported the following ways:

```
$ terraform import google_compute_disk.default projects/{{project}}/zones/{{zone}}/disks/{{diskname}}
$ terraform import google_compute_disk.default {{project}}/{{zone}}/{{instance.name}}:{{diskname}}
```

## » google\_\_compute\_\_autoscaler

Represents an Autoscaler resource.

Autoscalers allow you to automatically scale virtual machine instances in managed instance groups according to an autoscaling policy that you define.

To get more information about Autoscaler, see:

- API documentation
- How-to Guides
  - Autoscaling Groups of Instances



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Autoscaler Beta

```
resource "google_compute_autoscaler" "foobar" {
  provider = "google-beta"

  name      = "my-autoscaler"
  zone      = "us-central1-f"
  target    = "${google_compute_instance_group_manager.foobar.self_link}"

  autoscaling_policy {
    max_replicas    = 5
    min_replicas    = 1
    cooldown_period = 60

    cpu_utilization {
      target = 0.5
    }
  }
}

resource "google_compute_instance_template" "foobar" {
  provider = "google-beta"

  name          = "my-instance-template"
  machine_type  = "n1-standard-1"
  can_ip_forward = false

  tags = ["foo", "bar"]

  disk {
    source_image = "${data.google_compute_image.debian_9.self_link}"
  }

  network_interface {
    network = "default"
  }

  metadata = {
    foo = "bar"
  }
}
```

```

    }

    service_account {
      scopes = ["userinfo-email", "compute-ro", "storage-ro"]
    }
  }

  resource "google_compute_target_pool" "foobar" {
    provider = "google-beta"

    name = "my-target-pool"
  }

  resource "google_compute_instance_group_manager" "foobar" {
    provider = "google-beta"

    name = "my-igm"
    zone = "us-central1-f"

    version {
      instance_template = "${google_compute_instance_template.foobar.self_link}"
      name               = "primary"
    }

    target_pools      = ["${google_compute_target_pool.foobar.self_link}"]
    base_instance_name = "foobar"
  }

  data "google_compute_image" "debian_9" {
    provider = "google-beta"

    family = "debian-9"
    project = "debian-cloud"
  }

  provider "google-beta" {
    region = "us-central1"
    zone   = "us-central1-a"
  }

```



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Autoscaler Basic

```
resource "google_compute_autoscaler" "foobar" {
  name     = "my-autoscaler"
  zone     = "us-central1-f"
  target   = "${google_compute_instance_group_manager.foobar.self_link}"

  autoscaling_policy {
    max_replicas    = 5
    min_replicas    = 1
    cooldown_period = 60

    cpu_utilization {
      target = 0.5
    }
  }
}

resource "google_compute_instance_template" "foobar" {
  name          = "my-instance-template"
  machine_type  = "n1-standard-1"
  can_ip_forward = false

  tags = ["foo", "bar"]

  disk {
    source_image = "${data.google_compute_image.debian_9.self_link}"
  }

  network_interface {
    network = "default"
  }

  metadata = {
    foo = "bar"
  }

  service_account {
    scopes = ["userinfo-email", "compute-ro", "storage-ro"]
  }
}

resource "google_compute_target_pool" "foobar" {
  name = "my-target-pool"
}
```

```

resource "google_compute_instance_group_manager" "foobar" {
  name = "my-igm"
  zone = "us-central1-f"

  instance_template = "${google_compute_instance_template.foobar.self_link}"

  target_pools      = ["${google_compute_target_pool.foobar.self_link}"]
  base_instance_name = "foobar"
}

data "google_compute_image" "debian_9" {
  family = "debian-9"
  project = "debian-cloud"
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. The name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- **autoscaling\_policy** - (Required) The configuration parameters for the autoscaling algorithm. You can define one or more of the policies for an autoscaler: `cpuUtilization`, `customMetricUtilizations`, and `loadBalancingUtilization`. If none of these are specified, the default will be to autoscale based on `cpuUtilization` to 0.6 or 60%. Structure is documented below.
- **target** - (Required) URL of the managed instance group that this autoscaler will scale.

The `autoscaling_policy` block supports:

- **min\_replicas** - (Required) The minimum number of replicas that the autoscaler can scale down to. This cannot be less than 0. If not provided, autoscaler will choose a default value depending on maximum number of instances allowed.
- **max\_replicas** - (Required) The maximum number of instances that the autoscaler can scale up to. This is required when creating or updating an autoscaler. The maximum number of replicas should not be lower than minimal number of replicas.

- **cooldown\_period** - (Optional) The number of seconds that the autoscaler should wait before it starts collecting information from a new instance. This prevents the autoscaler from collecting information when the instance is initializing, during which the collected usage would not be reliable. The default time autoscaler waits is 60 seconds. Virtual machine initialization times might vary because of numerous factors. We recommend that you test how long an instance may take to initialize. To do this, create an instance and time the startup process.
- **cpu\_utilization** - (Optional) Defines the CPU utilization policy that allows the autoscaler to scale based on the average CPU utilization of a managed instance group. Structure is documented below.
- **metric** - (Optional) Defines the CPU utilization policy that allows the autoscaler to scale based on the average CPU utilization of a managed instance group. Structure is documented below.
- **load\_balancing\_utilization** - (Optional) Configuration parameters of autoscaling based on a load balancer. Structure is documented below.

The **cpu\_utilization** block supports:

- **target** - (Required) The target CPU utilization that the autoscaler should maintain. Must be a float value in the range (0, 1]. If not specified, the default is 0.6. If the CPU level is below the target utilization, the autoscaler scales down the number of instances until it reaches the minimum number of instances you specified or until the average CPU of your instances reaches the target utilization. If the average CPU is above the target utilization, the autoscaler scales up until it reaches the maximum number of instances you specified or until the average utilization reaches the target utilization.

The **metric** block supports:

- **name** - (Required) The identifier (type) of the Stackdriver Monitoring metric. The metric cannot have negative values. The metric must have a value type of INT64 or DOUBLE.
- **target** - (Required) The target value of the metric that autoscaler should maintain. This must be a positive value. A utilization metric scales number of virtual machines handling requests to increase or decrease proportionally to the metric. For example, a good metric to use as a utilization-Target is [www.googleapis.com/compute/instance/network/received\\_bytes\\_count](https://www.googleapis.com/compute/instance/network/received_bytes_count). The autoscaler will work to keep this value constant for each of the instances.
- **type** - (Required) Defines how target utilization value is expressed for a Stackdriver Monitoring metric. Either GAUGE, DELTA\_PER\_SECOND, or DELTA\_PER\_MINUTE.

- **filter** - (Optional, Beta) A filter string to be used as the filter string for a Stackdriver Monitoring TimeSeries.list API call. This filter is used to select a specific TimeSeries for the purpose of autoscaling and to determine whether the metric is exporting per-instance or per-group data. You can only use the AND operator for joining selectors. You can only use direct equality comparison operator (=) without any functions for each selector. You can specify the metric in both the filter string and in the metric field. However, if specified in both places, the metric must be identical. The monitored resource type determines what kind of values are expected for the metric. If it is a gce\_instance, the autoscaler expects the metric to include a separate TimeSeries for each instance in a group. In such a case, you cannot filter on resource labels. If the resource type is any other value, the autoscaler expects this metric to contain values that apply to the entire autoscaled instance group and resource label filtering can be performed to point autoscaler at the correct TimeSeries to scale upon. This is called a per-group metric for the purpose of autoscaling. If not specified, the type defaults to gce\_instance. You should provide a filter that is selective enough to pick just one TimeSeries for the autoscaled group or for each of the instances (if you are using gce\_instance resource type). If multiple TimeSeries are returned upon the query execution, the autoscaler will sum their respective values to obtain its scaling value.

The `load_balancing_utilization` block supports:

- **target** - (Required) Fraction of backend capacity utilization (set in HTTP(s) load balancing configuration) that autoscaler should maintain. Must be a positive float value. If not defined, the default is 0.8.
- 
- **description** - (Optional) An optional description of this resource.
  - **zone** - (Optional) URL of the zone where the instance group resides.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **self\_link** - The URI of the created resource.



## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Autoscaler can be imported using any of these accepted formats:

```
$ terraform import google_compute_autoscaler.default projects/{{project}}/zones/{{zone}}/autoscalers/{{name}}
$ terraform import google_compute_autoscaler.default {{zone}}/{{name}}
$ terraform import google_compute_autoscaler.default {{project}}/{{zone}}/{{name}}
$ terraform import google_compute_autoscaler.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_backend\_bucket

Backend buckets allow you to use Google Cloud Storage buckets with HTTP(S) load balancing.

An HTTP(S) load balancer can direct traffic to specified URLs to a backend bucket rather than a backend service. It can send requests for static content to a Cloud Storage bucket and requests for dynamic content a virtual machine instance.

To get more information about BackendBucket, see:

- API documentation
- How-to Guides
  - Using a Cloud Storage bucket as a load balancer backend



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Backend Bucket Basic

```
resource "google_compute_backend_bucket" "image_backend" {
```

```

    name          = "image-backend-bucket"
    description    = "Contains beautiful images"
    bucket_name    = "${google_storage_bucket.image_bucket.name}"
    enable_cdn     = true
  }

  resource "google_storage_bucket" "image_bucket" {
    name          = "image-store-bucket"
    location      = "EU"
  }

```

## » Argument Reference

The following arguments are supported:

- **bucket\_name** - (Required) Cloud Storage bucket name.
  - **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- 
- **description** - (Optional) An optional textual description of the resource; provided by the client when the resource is created.
  - **enable\_cdn** - (Optional) If true, enable Cloud CDN for this Backend-Bucket.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

BackendBucket can be imported using any of these accepted formats:

```
$ terraform import google_compute_backend_bucket.default projects/{{project}}/global/backend
$ terraform import google_compute_backend_bucket.default {{project}}/{{name}}
$ terraform import google_compute_backend_bucket.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_backend\_service

A Backend Service defines a group of virtual machines that will serve traffic for load balancing. For more information see the official documentation and the API.

For internal load balancing, use a `google_compute_region_backend_service`.

## » Example Usage

```
resource "google_compute_backend_service" "website" {
  name          = "my-backend"
  description   = "Our company website"
  port_name     = "http"
  protocol      = "HTTP"
  timeout_sec   = 10
  enable_cdn    = false

  backend {
    group = "${google_compute_instance_group_manager.webservers.instance_group}"
  }

  health_checks = ["${google_compute_http_health_check.default.self_link}"]
}

resource "google_compute_instance_group_manager" "webservers" {
  name          = "my-webservers"
  instance_template = "${google_compute_instance_template.webserver.self_link}"
}
```

```

    base_instance_name = "webserver"
    zone               = "us-central1-f"
    target_size        = 1
  }

  resource "google_compute_instance_template" "webserver" {
    name          = "standard-webserver"
    machine_type  = "n1-standard-1"

    network_interface {
      network = "default"
    }

    disk {
      source_image = "debian-cloud/debian-9"
      auto_delete  = true
      boot         = true
    }
  }

  resource "google_compute_http_health_check" "default" {
    name          = "test"
    request_path   = "/"
    check_interval_sec = 1
    timeout_sec    = 1
  }

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the backend service.
  - **health\_checks** - (Required) Specifies a list of HTTP/HTTPS health checks for checking the health of the backend service. Currently at most one health check can be specified, and a health check is required.
- 
- **backend** - (Optional) The list of backends that serve this BackendService. Structure is documented below.
  - **iap** - (Optional) Specification for the Identity-Aware proxy. Disabled if not specified. Structure is documented below.
  - **cdn\_policy** - (Optional) Cloud CDN configuration for this BackendService. Structure is documented below.

- **connection\_draining\_timeout\_sec** - (Optional) Time for which instance will be drained (not accept new connections, but still work to finish started ones). Defaults to 300.
- **custom\_request\_headers** - (Optional, Beta) Headers that the HTTP/S load balancer should add to proxied requests. See guide for details.
- **description** - (Optional) The textual description for the backend service.
- **enable\_cdn** - (Optional) Whether or not to enable the Cloud CDN on the backend service.
- **port\_name** - (Optional) The name of a service that has been added to an instance group in this backend. See related docs for details. Defaults to http.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **protocol** - (Optional) The protocol for incoming requests. Defaults to HTTP.
- **security\_policy** - (Optional) Name or URI of a security policy to add to the backend service.
- **session\_affinity** - (Optional) How to distribute load. Options are NONE (no affinity), CLIENT\_IP (hash of the source/dest addresses / ports), and GENERATED\_COOKIE (distribute load using a generated session cookie).
- **affinity\_cookie\_ttl\_sec** - (Optional) Lifetime of cookies in seconds if session\_affinity is GENERATED\_COOKIE. If set to 0, the cookie is non-persistent and lasts only until the end of the browser session (or equivalent). The maximum allowed value for TTL is one day.
- **timeout\_sec** - (Optional) The number of secs to wait for a backend to respond to a request before considering the request failed. Defaults to 30.

The **backend** block supports:

- **group** - (Required) The name or URI of a Compute Engine instance group (`google_compute_instance_group_manager.xyz.instance_group`) that can receive traffic.
- **balancing\_mode** - (Optional) Defines the strategy for balancing load. Defaults to UTILIZATION
- **capacity\_scaler** - (Optional) A float in the range [0, 1.0] that scales the maximum parameters for the group (e.g., max rate). A value of 0.0 will cause no requests to be sent to the group (i.e., it adds the group in a drained state). The default is 1.0.
- **description** - (Optional) Textual description for the backend.

- **max\_rate** - (Optional) Maximum requests per second (RPS) that the group can handle.
- **max\_rate\_per\_instance** - (Optional) The maximum per-instance requests per second (RPS).
- **max\_connections** - (Optional) The max number of simultaneous connections for the group. Can be used with either CONNECTION or UTILIZATION balancing modes. For CONNECTION mode, either maxConnections or maxConnectionsPerInstance must be set.
- **max\_connections\_per\_instance** - (Optional) The max number of simultaneous connections that a single backend instance can handle. This is used to calculate the capacity of the group. Can be used in either CONNECTION or UTILIZATION balancing modes. For CONNECTION mode, either maxConnections or maxConnectionsPerInstance must be set.
- **max\_utilization** - (Optional) The target CPU utilization for the group as a float in the range [0.0, 1.0]. This flag can only be provided when the balancing mode is UTILIZATION. Defaults to 0.8.

The **cdn\_policy** block supports:

- **cache\_key\_policy** - (Optional) The CacheKeyPolicy for this CdnPolicy. Structure is documented below.

The **cache\_key\_policy** block supports:

- **include\_host** - (Optional) If true, requests to different hosts will be cached separately.
- **include\_protocol** - (Optional) If true, http and https requests will be cached separately.
- **include\_query\_string** - (Optional) If true, include query string parameters in the cache key according to **query\_string\_whitelist** and **query\_string\_blacklist**. If neither is set, the entire query string will be included. If false, the query string will be excluded from the cache key entirely.
- **query\_string\_blacklist** - (Optional) Names of query string parameters to exclude in cache keys. All other parameters will be included. Either specify **query\_string\_whitelist** or **query\_string\_blacklist**, not both. '&' and '=' will be percent encoded and not treated as delimiters.
- **query\_string\_whitelist** - (Optional) Names of query string parameters to include in cache keys. All other parameters will be excluded. Either specify **query\_string\_whitelist** or **query\_string\_blacklist**, not both. '&' and '=' will be percent encoded and not treated as delimiters.

The **iap** block supports:

- **oauth2\_client\_id** - (Required) The client ID for use with OAuth 2.0.

- `oauth2_client_secret` - (Required) The client secret for use with OAuth 2.0. Out of band changes to this field will not be detected by Terraform, and it may perform spurious no-op updates when imported, or upgraded from pre-2.0.0.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `iap.0.oauth2_client_secret_sha256` - The SHA256 hash of the OAuth 2.0 client secret value.
- `fingerprint` - The fingerprint of the backend service.
- `self_link` - The URI of the created resource.

## » Import

Backend services can be imported using the `name`, e.g.

```
$ terraform import google_compute_backend_service.website my-backend
```

## » google\_\_compute\_\_disk

Persistent disks are durable storage devices that function similarly to the physical disks in a desktop or a server. Compute Engine manages the hardware behind these devices to ensure data redundancy and optimize performance for you. Persistent disks are available as either standard hard disk drives (HDD) or solid-state drives (SSD).

Persistent disks are located independently from your virtual machine instances, so you can detach or move persistent disks to keep your data even after you delete your instances. Persistent disk performance scales automatically with size, so you can resize your existing persistent disks or add more persistent disks to an instance to meet your performance and storage space requirements.

Add a persistent disk to your instance when you need reliable and affordable storage with consistent performance characteristics.

To get more information about Disk, see:

- API documentation
- How-to Guides
  - Adding a persistent disk

**Warning:** All arguments including the disk encryption key will be stored in the raw state as plain-text. Read more about sensitive data in state.



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Disk Basic

```
resource "google_compute_disk" "default" {
  name = "test-disk"
  type = "pd-ssd"
  zone = "us-central1-a"
  image = "debian-8-jessie-v20170523"
  labels = {
    environment = "dev"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.
- **labels** - (Optional) Labels to apply to this disk. A list of key->value pairs.
- **size** - (Optional) Size of the persistent disk, specified in GB. You can specify this field when creating a persistent disk using the `sourceImage` or `sourceSnapshot` parameter, or specify it alone to create an empty persistent disk. If you specify this field along with `sourceImage` or `sourceSnapshot`, the value of `sizeGb` must not be less than the size of the `sourceImage` or the size of the snapshot.



- **type** - (Optional) URL of the disk type resource describing which disk type to use to create the disk. Provide this when creating the disk.
- **image** - (Optional) The image from which to initialize this disk. This can be one of: the image's `self_link`, `projects/{project}/global/images/{image}`, `projects/{project}/global/images/family/{family}`, `global/images/{image}`, `global/images/family/{family}`, `family/{family}`, `{project}/{family}`, `{project}/{image}`, `{family}`, or `{image}`. If referred by family, the images names must include the family name. If they don't, use the `google_compute_image` data source. For instance, the image `centos-6-v20180104` includes its family name `centos-6`. These images can be referred by family name here.
- **zone** - (Optional) A reference to the zone where the disk resides.
- **source\_image\_encryption\_key** - (Optional) The customer-supplied encryption key of the source image. Required if the source image is protected by a customer-supplied encryption key. Structure is documented below.
- **disk\_encryption\_key** - (Optional) Encrypts the disk using a customer-supplied encryption key. After you encrypt a disk with a customer-supplied key, you must provide the same key if you use the disk later (e.g. to create a disk snapshot or an image, or to attach the disk to a virtual machine). Customer-supplied encryption keys do not protect access to metadata of the disk. If you do not provide an encryption key when creating the disk, then the disk will be encrypted using an automatically generated key and you do not need to provide a key to use the disk later. Structure is documented below.
- **snapshot** - (Optional) The source snapshot used to create this disk. You can provide this as a partial or full URL to the resource. For example, the following are valid values:
  - `https://www.googleapis.com/compute/v1/projects/project/global/snapshots/snapshot`
  - `projects/project/global/snapshots/snapshot`
  - `global/snapshots/snapshot`
  - `snapshot`
- **source\_snapshot\_encryption\_key** - (Optional) The customer-supplied encryption key of the source snapshot. Required if the source snapshot is protected by a customer-supplied encryption key. Structure is documented below.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The `source_image_encryption_key` block supports:

- **raw\_key** - (Optional) Specifies a 256-bit customer-supplied encryption key, encoded in RFC 4648 base64 to either encrypt or decrypt this resource.

- **sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.
- **kms\_key\_self\_link** - (Optional) The self link of the encryption key used to encrypt the disk. Also called KmsKeyName in the cloud console. In order to use this additional IAM permissions need to be set on the Compute Engine Service Agent. See [https://cloud.google.com/compute/docs/disks/customer-managed-encryption#encrypt\\_a\\_new\\_persistent\\_disk\\_with\\_your\\_own\\_keys](https://cloud.google.com/compute/docs/disks/customer-managed-encryption#encrypt_a_new_persistent_disk_with_your_own_keys)

The **disk\_encryption\_key** block supports:

- **raw\_key** - (Optional) Specifies a 256-bit customer-supplied encryption key, encoded in RFC 4648 base64 to either encrypt or decrypt this resource.
- **sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.
- **kms\_key\_self\_link** - (Optional) The self link of the encryption key used to encrypt the disk. Also called KmsKeyName in the cloud console. In order to use this additional IAM permissions need to be set on the Compute Engine Service Agent. See [https://cloud.google.com/compute/docs/disks/customer-managed-encryption#encrypt\\_a\\_new\\_persistent\\_disk\\_with\\_your\\_own\\_keys](https://cloud.google.com/compute/docs/disks/customer-managed-encryption#encrypt_a_new_persistent_disk_with_your_own_keys)

The **source\_snapshot\_encryption\_key** block supports:

- **raw\_key** - (Optional) Specifies a 256-bit customer-supplied encryption key, encoded in RFC 4648 base64 to either encrypt or decrypt this resource.
- **kms\_key\_self\_link** - (Optional) The self link of the encryption key used to encrypt the disk. Also called KmsKeyName in the cloud console. In order to use this additional IAM permissions need to be set on the Compute Engine Service Agent. See [https://cloud.google.com/compute/docs/disks/customer-managed-encryption#encrypt\\_a\\_new\\_persistent\\_disk\\_with\\_your\\_own\\_keys](https://cloud.google.com/compute/docs/disks/customer-managed-encryption#encrypt_a_new_persistent_disk_with_your_own_keys)
- **sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **label\_fingerprint** - The fingerprint used for optimistic locking of this resource. Used internally during updates.
- **creation\_timestamp** - Creation timestamp in RFC3339 text format.

- `last_attach_timestamp` - Last attach timestamp in RFC3339 text format.
- `last_detach_timestamp` - Last detach timestamp in RFC3339 text format.
- `users` - Links to the users of the disk (attached instances) in form: `project/zones/zone/instances/instance`
- `source_image_id` - The ID value of the image used to create this disk. This value identifies the exact image that was used to create this persistent disk. For example, if you created the persistent disk from an image that was later deleted and recreated under the same name, the source image ID would identify the exact version of the image that was used.
- `source_snapshot_id` - The unique ID of the snapshot used to create this disk. This value identifies the exact snapshot that was used to create this persistent disk. For example, if you created the persistent disk from a snapshot that was later deleted and recreated under the same name, the source snapshot ID would identify the exact version of the snapshot that was used.
- `self_link` - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 5 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Disk can be imported using any of these accepted formats:

```
$ terraform import google_compute_disk.default projects/{{project}}/zones/{{zone}}/disks/{{name}}
$ terraform import google_compute_disk.default {{project}}/{{zone}}/{{name}}
$ terraform import google_compute_disk.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_firewall

Each network has its own firewall controlling access to and from the instances.

All traffic to instances, even from other instances, is blocked by the firewall unless firewall rules are created to allow it.

The default network has automatically created firewall rules that are shown in default firewall rules. No manually created network has automatically created firewall rules except for a default "allow" rule for outgoing traffic and a default "deny" for incoming traffic. For all networks except the default network, you must create any firewall rules you need.

To get more information about Firewall, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Firewall Basic

```
resource "google_compute_firewall" "default" {
  name      = "test-firewall"
  network   = "${google_compute_network.default.name}"

  allow {
    protocol = "icmp"
  }

  allow {
    protocol = "tcp"
    ports    = ["80", "8080", "1000-2000"]
  }

  source_tags = ["web"]
}

resource "google_compute_network" "default" {
  name = "test-network"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
  - **network** - (Required) The name or `self_link` of the network to attach this firewall to.
- 
- **allow** - (Optional) The list of ALLOW rules specified by this firewall. Each rule specifies a protocol and port-range tuple that describes a permitted connection. Structure is documented below.
  - **deny** - (Optional) The list of DENY rules specified by this firewall. Each rule specifies a protocol and port-range tuple that describes a denied connection. Structure is documented below.
  - **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.
  - **destination\_ranges** - (Optional) If destination ranges are specified, the firewall will apply only to traffic that has destination IP address in these ranges. These ranges must be expressed in CIDR format. Only IPv4 is supported.
  - **direction** - (Optional) Direction of traffic to which this firewall applies; default is INGRESS. Note: For INGRESS traffic, it is NOT supported to specify `destinationRanges`; For EGRESS traffic, it is NOT supported to specify `sourceRanges` OR `sourceTags`.
  - **disabled** - (Optional) Denotes whether the firewall rule is disabled, i.e not applied to the network it is associated with. When set to true, the firewall rule is not enforced and the network behaves as if it did not exist. If this is unspecified, the firewall rule will be enabled.
  - **enable\_logging** - (Optional, Beta) This field denotes whether to enable logging for a particular firewall rule. If logging is enabled, logs will be exported to Stackdriver.
  - **priority** - (Optional) Priority for this rule. This is an integer between 0 and 65535, both inclusive. When not specified, the value assumed is 1000. Relative priorities determine precedence of conflicting rules. Lower value of priority implies higher precedence (eg, a rule with priority 0 has higher

precedence than a rule with priority 1). DENY rules take precedence over ALLOW rules having equal priority.

- **source\_ranges** - (Optional) If source ranges are specified, the firewall will apply only to traffic that has source IP address in these ranges. These ranges must be expressed in CIDR format. One or both of `sourceRanges` and `sourceTags` may be set. If both properties are set, the firewall will apply to traffic that has source IP address within `sourceRanges` OR the source IP that belongs to a tag listed in the `sourceTags` property. The connection does not need to match both properties for the firewall to apply. Only IPv4 is supported.
- **source\_service\_accounts** - (Optional) If source service accounts are specified, the firewall will apply only to traffic originating from an instance with a service account in this list. Source service accounts cannot be used to control traffic to an instance's external IP address because service accounts are associated with an instance, not an IP address. `sourceRanges` can be set at the same time as `sourceServiceAccounts`. If both are set, the firewall will apply to traffic that has source IP address within `sourceRanges` OR the source IP belongs to an instance with service account listed in `sourceServiceAccount`. The connection does not need to match both properties for the firewall to apply. `sourceServiceAccounts` cannot be used at the same time as `sourceTags` or `targetTags`.
- **source\_tags** - (Optional) If source tags are specified, the firewall will apply only to traffic with source IP that belongs to a tag listed in `sourceTags`. Source tags cannot be used to control traffic to an instance's external IP address. Because tags are associated with an instance, not an IP address. One or both of `sourceRanges` and `sourceTags` may be set. If both properties are set, the firewall will apply to traffic that has source IP address within `sourceRanges` OR the source IP that belongs to a tag listed in the `sourceTags` property. The connection does not need to match both properties for the firewall to apply.
- **target\_service\_accounts** - (Optional) A list of service accounts indicating sets of instances located in the network that may make network connections as specified in `allowed[]`. `targetServiceAccounts` cannot be used at the same time as `targetTags` or `sourceTags`. If neither `targetServiceAccounts` nor `targetTags` are specified, the firewall rule applies to all instances on the specified network.
- **target\_tags** - (Optional) A list of instance tags indicating sets of instances located in the network that may make network connections as specified in `allowed[]`. If no `targetTags` are specified, the firewall rule applies to all instances on the specified network.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **allow** block supports:

- **protocol** - (Required) The IP protocol to which this rule applies. The protocol type is required when creating a firewall rule. This value can either be one of the following well known protocol strings (tcp, udp, icmp, esp, ah, sctp), or the IP protocol number.
- **ports** - (Optional) An optional list of ports to which this rule applies. This field is only applicable for UDP or TCP protocol. Each entry must be either an integer or a range. If not specified, this rule applies to connections through any port. Example inputs include: ["22"], ["80","443"], and ["12345-12349"].

The **deny** block supports:

- **protocol** - (Required) The IP protocol to which this rule applies. The protocol type is required when creating a firewall rule. This value can either be one of the following well known protocol strings (tcp, udp, icmp, esp, ah, sctp), or the IP protocol number.
- **ports** - (Optional) An optional list of ports to which this rule applies. This field is only applicable for UDP or TCP protocol. Each entry must be either an integer or a range. If not specified, this rule applies to connections through any port. Example inputs include: ["22"], ["80","443"], and ["12345-12349"].

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

Firewall can be imported using any of these accepted formats:

```
$ terraform import google_compute_firewall.default projects/{{project}}/global/firewalls/{{name}}
$ terraform import google_compute_firewall.default {{project}}/{{name}}
$ terraform import google_compute_firewall.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_compute_forwarding_rule`

A `ForwardingRule` resource. A `ForwardingRule` resource specifies which pool of target virtual machines to forward a packet to if it matches the given `[IPAddress, IPProtocol, portRange]` tuple.

To get more information about `ForwardingRule`, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Forwarding Rule Basic

```
resource "google_compute_forwarding_rule" "default" {
  name      = "website-forwarding-rule"
  target    = "${google_compute_target_pool.default.self_link}"
  port_range = "80"
}

resource "google_compute_target_pool" "default" {
  name = "website-target-pool"
}
```

## » Argument Reference

The following arguments are supported:

- `name` - (Required) Name of the resource; provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long



and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

- 
- **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.
  - **ip\_address** - (Optional) The IP address that this forwarding rule is serving on behalf of. Addresses are restricted based on the forwarding rule's load balancing scheme (EXTERNAL or INTERNAL) and scope (global or regional). When the load balancing scheme is EXTERNAL, for global forwarding rules, the address must be a global IP, and for regional forwarding rules, the address must live in the same region as the forwarding rule. If this field is empty, an ephemeral IPv4 address from the same scope (global or regional) will be assigned. A regional forwarding rule supports IPv4 only. A global forwarding rule supports either IPv4 or IPv6. When the load balancing scheme is INTERNAL, this can only be an RFC 1918 IP address belonging to the network/subnet configured for the forwarding rule. By default, if this field is empty, an ephemeral internal IP address will be automatically allocated from the IP range of the subnet or network configured for this forwarding rule. An address can be specified either by a literal IP address or a URL reference to an existing Address resource. The following examples are all valid:
    - 100.1.2.3
    - <https://www.googleapis.com/compute/v1/projects/project/regions/region/addresses/address>
    - [projects/project/regions/region/addresses/address](https://www.googleapis.com/compute/v1/projects/project/regions/region/addresses/address)
    - [regions/region/addresses/address](https://www.googleapis.com/compute/v1/projects/project/regions/region/addresses/address)
    - [global/addresses/address](https://www.googleapis.com/compute/v1/projects/project/regions/region/addresses/address)
    - [address](https://www.googleapis.com/compute/v1/projects/project/regions/region/addresses/address)
  - **ip\_protocol** - (Optional) The IP protocol to which this rule applies. Valid options are TCP, UDP, ESP, AH, SCTP or ICMP. When the load balancing scheme is INTERNAL, only TCP and UDP are valid.
  - **backend\_service** - (Optional) A reference to a BackendService to receive the matched traffic. This is used for internal load balancing. (not used for external load balancing)
  - **ip\_version** - (Optional) The IP Version that will be used by this forwarding rule. Valid options are IPV4 or IPV6. This can only be specified for a global forwarding rule.
  - **load\_balancing\_scheme** - (Optional) This signifies what the ForwardingRule will be used for and can only take the following values: INTERNAL, EXTERNAL. The value of INTERNAL means that this will be used

for Internal Network Load Balancing (TCP, UDP). The value of EXTERNAL means that this will be used for External Load Balancing (HTTP(S) LB, External TCP/UDP LB, SSL Proxy)

- **network** - (Optional) For internal load balancing, this field identifies the network that the load balanced IP should belong to for this Forwarding Rule. If this field is not specified, the default network will be used. This field is not used for external load balancing.
- **port\_range** - (Optional) This field is used along with the target field for TargetHttpProxy, TargetHttpsProxy, TargetSslProxy, TargetTcpProxy, TargetVpnGateway, TargetPool, TargetInstance. Applicable only when IPProtocol is TCP, UDP, or SCTP, only packets addressed to ports in the specified range will be forwarded to target. Forwarding rules with the same [IPAddress, IPProtocol] pair must have disjoint port ranges. Some types of forwarding target have constraints on the acceptable ports:
  - TargetHttpProxy: 80, 8080
  - TargetHttpsProxy: 443
  - TargetTcpProxy: 25, 43, 110, 143, 195, 443, 465, 587, 700, 993, 995, 1883, 5222
  - TargetSslProxy: 25, 43, 110, 143, 195, 443, 465, 587, 700, 993, 995, 1883, 5222
  - TargetVpnGateway: 500, 4500
- **ports** - (Optional) This field is used along with the backend\_service field for internal load balancing. When the load balancing scheme is INTERNAL, a single port or a comma separated list of ports can be configured. Only packets addressed to these ports will be forwarded to the backends configured with this forwarding rule. You may specify a maximum of up to 5 ports.
- **subnetwork** - (Optional) A reference to a subnetwork. For internal load balancing, this field identifies the subnetwork that the load balanced IP should belong to for this Forwarding Rule. If the network specified is in auto subnet mode, this field is optional. However, if the network is in custom subnet mode, a subnetwork must be specified. This field is not used for external load balancing.
- **target** - (Optional) A reference to a TargetPool resource to receive the matched traffic. For regional forwarding rules, this target must live in the same region as the forwarding rule. For global forwarding rules, this target must be a global load balancing resource. The forwarded traffic must be of a type appropriate to the target object. This field is not used for internal load balancing.
- **labels** - (Optional, Beta) Labels to apply to this forwarding rule. A list of key->value pairs.

- **all\_ports** - (Optional, Beta) When the load balancing scheme is INTERNAL and protocol is TCP/UDP, omit **port/port\_range** and specify this field as **true** to allow packets addressed to any ports to be forwarded to the backends configured with this forwarding rule.
- **network\_tier** - (Optional) The networking tier used for configuring this address. This field can take the following values: PREMIUM or STANDARD. If this field is not specified, it is assumed to be PREMIUM.
- **service\_label** - (Optional, Beta) An optional prefix to the service name for this Forwarding Rule. If specified, will be the first label of the fully qualified service name. The label must be 1-63 characters long, and comply with RFC1035. Specifically, the label must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash. This field is only used for internal load balancing.
- **region** - (Optional) A reference to the region where the regional forwarding rule resides. This field is not applicable to global forwarding rules.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **label\_fingerprint** - The fingerprint used for optimistic locking of this resource. Used internally during updates.
- **service\_name** - The internal fully qualified service name for this Forwarding Rule. This field is only used for internal load balancing.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

ForwardingRule can be imported using any of these accepted formats:

```
$ terraform import google_compute_forwarding_rule.default projects/{{project}}/regions/{{region}}/forwarding_rules/{{name}}
$ terraform import google_compute_forwarding_rule.default {{project}}/{{region}}/{{name}}
$ terraform import google_compute_forwarding_rule.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_global\_address

Represents a Global Address resource. Global addresses are used for HTTP(S) load balancing.

To get more information about GlobalAddress, see:

- API documentation
- How-to Guides
  - Reserving a Static External IP Address



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Global Address Basic

```
resource "google_compute_global_address" "default" {
  name = "global-appserver-ip"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

- 
- **address** - (Optional) The static external IP address represented by this resource.
  - **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.
  - **labels** - (Optional, Beta) Labels to apply to this address. A list of key->value pairs.
  - **ip\_version** - (Optional) The IP Version that will be used by this address. Valid options are IPV4 or IPV6. The default value is IPV4.
  - **prefix\_length** - (Optional, Beta) The prefix length of the IP range. If not present, it means the address field is a single IP address. This field is not applicable to addresses with addressType=EXTERNAL.
  - **address\_type** - (Optional) The type of the address to reserve, default is EXTERNAL.
    - EXTERNAL indicates public/external single IP address.
    - INTERNAL indicates internal IP ranges belonging to some network.
  - **purpose** - (Optional, Beta) The purpose of the resource. For global internal addresses it can be
    - VPC\_PEERING - for peer networks This should only be set when using an Internal address.
  - **network** - (Optional, Beta) The URL of the network in which to reserve the IP range. The IP range must be in RFC1918 space. The network cannot be deleted if there are any reserved IP ranges referring to it. This should only be set when using an Internal address.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **label\_fingerprint** - The fingerprint used for optimistic locking of this resource. Used internally during updates.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

GlobalAddress can be imported using any of these accepted formats:

```
$ terraform import google_compute_global_address.default projects/{{project}}/global/address/{{name}}
$ terraform import google_compute_global_address.default {{project}}/{{name}}
$ terraform import google_compute_global_address.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_global\_forwarding\_rule

Manages a Global Forwarding Rule within GCE. This binds an ip and port to a target HTTP(s) proxy. For more information see the official documentation and API.

## » Example Usage

```
resource "google_compute_global_forwarding_rule" "default" {
  name      = "default-rule"
  target    = "${google_compute_target_http_proxy.default.self_link}"
  port_range = "80"
}

resource "google_compute_target_http_proxy" "default" {
  name          = "test-proxy"
  description   = "a description"
  url_map       = "${google_compute_url_map.default.self_link}"
}

resource "google_compute_url_map" "default" {
  name          = "url-map"
  description   = "a description"
  default_service = "${google_compute_backend_service.default.self_link}"
}
```

```

host_rule {
  hosts      = ["mysite.com"]
  path_matcher = "allpaths"
}

path_matcher {
  name          = "allpaths"
  default_service = "${google_compute_backend_service.default.self_link}"

  path_rule {
    paths      = ["/*"]
    service = "${google_compute_backend_service.default.self_link}"
  }
}

resource "google_compute_backend_service" "default" {
  name          = "default-backend"
  port_name     = "http"
  protocol      = "HTTP"
  timeout_sec   = 10

  health_checks = ["${google_compute_http_health_check.default.self_link}"]
}

resource "google_compute_http_health_check" "default" {
  name          = "test"
  request_path   = "/"
  check_interval_sec = 1
  timeout_sec    = 1
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique name for the resource, required by GCE. Changing this forces a new resource to be created.
  - **target** - (Required) URL of target HTTP or HTTPS proxy.
- 
- **description** - (Optional) Textual description field.
  - **ip\_address** - (Optional) The static IP. (if not set, an ephemeral IP

is used). This should be the literal IP address to be used, not the `self_link` to a `google_compute_global_address` resource. (If using a `google_compute_global_address` resource, use the `address` property instead of the `self_link` property.)

- `ip_protocol` - (Optional) The IP protocol to route, one of "TCP" "UDP" "AH" "ESP" or "SCTP". (default "TCP").
- `port_range` - (Optional) A range e.g. "1024-2048" or a single port "1024" (defaults to all ports!). Some types of forwarding targets have constraints on the acceptable ports:
  - Target HTTP proxy: 80, 8080
  - Target HTTPS proxy: 443
  - Target TCP proxy: 25, 43, 110, 143, 195, 443, 465, 587, 700, 993, 995, 1883, 5222
  - Target SSL proxy: 25, 43, 110, 143, 195, 443, 465, 587, 700, 993, 995, 1883, 5222
  - Target VPN gateway: 500, 4500
- `project` - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- `ip_version` - (Optional) The IP Version that will be used by this resource's address. One of "IPV4" or "IPV6". You cannot provide this and `ip_address`.

- 
- `labels` - (Optional, Beta) A set of key/value label pairs to assign to the resource.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `self_link` - The URI of the created resource.
- `label_fingerprint` (Beta) - The current label fingerprint.

## » Import

Global forwarding rules can be imported using the `name`, e.g.

```
$ terraform import google_compute_global_forwarding_rule.default default-rule
```



## » google\_compute\_health\_check

Health Checks determine whether instances are responsive and able to do work. They are an important part of a comprehensive load balancing configuration, as they enable monitoring instances behind load balancers.

Health Checks poll instances at a specified interval. Instances that do not respond successfully to some number of probes in a row are marked as unhealthy. No new connections are sent to unhealthy instances, though existing connections will continue. The health check will continue to poll unhealthy instances. If an instance later responds successfully to some number of consecutive probes, it is marked healthy again and can receive new connections.

To get more information about HealthCheck, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Health Check Basic

```
resource "google_compute_health_check" "internal-health-check" {
  name = "internal-service-health-check"

  timeout_sec          = 1
  check_interval_sec = 1

  tcp_health_check {
    port = "80"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which

means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

- 
- **check\_interval\_sec** - (Optional) How often (in seconds) to send a health check. The default value is 5 seconds.
  - **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.
  - **healthy\_threshold** - (Optional) A so-far unhealthy instance will be marked healthy after this many consecutive successes. The default value is 2.
  - **timeout\_sec** - (Optional) How long (in seconds) to wait before claiming failure. The default value is 5 seconds. It is invalid for timeoutSec to have greater value than checkIntervalSec.
  - **unhealthy\_threshold** - (Optional) A so-far healthy instance will be marked unhealthy after this many consecutive failures. The default value is 2.
  - **http\_health\_check** - (Optional) A nested object resource Structure is documented below.
  - **https\_health\_check** - (Optional) A nested object resource Structure is documented below.
  - **tcp\_health\_check** - (Optional) A nested object resource Structure is documented below.
  - **ssl\_health\_check** - (Optional) A nested object resource Structure is documented below.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **http\_health\_check** block supports:

- **host** - (Optional) The value of the host header in the HTTP health check request. If left empty (default value), the public IP on behalf of which this health check is performed will be used.
- **request\_path** - (Optional) The request path of the HTTP health check request. The default value is `/`.
- **response** - (Optional) The bytes to match against the beginning of the response data. If left empty (the default value), any response will indicate health. The response data can only be ASCII.
- **port** - (Optional) The TCP port number for the HTTP health check request. The default value is 80.

- **proxy\_header** - (Optional) Specifies the type of proxy header to append before sending data to the backend, either NONE or PROXY\_V1. The default is NONE.

The **https\_health\_check** block supports:

- **host** - (Optional) The value of the host header in the HTTPS health check request. If left empty (default value), the public IP on behalf of which this health check is performed will be used.
- **request\_path** - (Optional) The request path of the HTTPS health check request. The default value is /.
- **response** - (Optional) The bytes to match against the beginning of the response data. If left empty (the default value), any response will indicate health. The response data can only be ASCII.
- **port** - (Optional) The TCP port number for the HTTPS health check request. The default value is 443.
- **proxy\_header** - (Optional) Specifies the type of proxy header to append before sending data to the backend, either NONE or PROXY\_V1. The default is NONE.

The **tcp\_health\_check** block supports:

- **request** - (Optional) The application data to send once the TCP connection has been established (default value is empty). If both request and response are empty, the connection establishment alone will indicate health. The request data can only be ASCII.
- **response** - (Optional) The bytes to match against the beginning of the response data. If left empty (the default value), any response will indicate health. The response data can only be ASCII.
- **port** - (Optional) The TCP port number for the TCP health check request. The default value is 443.
- **proxy\_header** - (Optional) Specifies the type of proxy header to append before sending data to the backend, either NONE or PROXY\_V1. The default is NONE.

The **ssl\_health\_check** block supports:

- **request** - (Optional) The application data to send once the SSL connection has been established (default value is empty). If both request and response are empty, the connection establishment alone will indicate health. The request data can only be ASCII.
- **response** - (Optional) The bytes to match against the beginning of the response data. If left empty (the default value), any response will indicate health. The response data can only be ASCII.

- **port** - (Optional) The TCP port number for the SSL health check request. The default value is 443.
- **proxy\_header** - (Optional) Specifies the type of proxy header to append before sending data to the backend, either NONE or PROXY\_V1. The default is NONE.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **type** - The type of the health check. One of HTTP, HTTPS, TCP, or SSL.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

HealthCheck can be imported using any of these accepted formats:

```
$ terraform import google_compute_health_check.default projects/{{project}}/global/healthCheck/{{name}}
$ terraform import google_compute_health_check.default {{project}}/{{name}}
$ terraform import google_compute_health_check.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_http\_health\_check

An HttpHealthCheck resource. This resource defines a template for how individual VMs should be checked for health, via HTTP.

**Note:** `google_compute_http_health_check` is a legacy health check. The newer `google_compute_health_check` should be preferred for all uses except Network Load Balancers which still require the legacy version.

To get more information about `HttpHealthCheck`, see:

- API documentation
- How-to Guides
  - Adding Health Checks



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Http Health Check Basic

```
resource "google_compute_http_health_check" "default" {
  name          = "authentication-health-check"
  request_path  = "/health_check"

  timeout_sec      = 1
  check_interval_sec = 1
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- 
- **check\_interval\_sec** - (Optional) How often (in seconds) to send a health check. The default value is 5 seconds.
  - **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.

- **healthy\_threshold** - (Optional) A so-far unhealthy instance will be marked healthy after this many consecutive successes. The default value is 2.
- **host** - (Optional) The value of the host header in the HTTP health check request. If left empty (default value), the public IP on behalf of which this health check is performed will be used.
- **port** - (Optional) The TCP port number for the HTTP health check request. The default value is 80.
- **request\_path** - (Optional) The request path of the HTTP health check request. The default value is `/`.
- **timeout\_sec** - (Optional) How long (in seconds) to wait before claiming failure. The default value is 5 seconds. It is invalid for `timeoutSec` to have greater value than `checkIntervalSec`.
- **unhealthy\_threshold** - (Optional) A so-far healthy instance will be marked unhealthy after this many consecutive failures. The default value is 2.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

`HttpHealthCheck` can be imported using any of these accepted formats:

```
$ terraform import google_compute_http_health_check.default projects/{{project}}/global/httpHealthCheck/{{name}}
$ terraform import google_compute_http_health_check.default {{project}}/{{name}}
$ terraform import google_compute_http_health_check.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_compute_https_health_check`

An `HttpsHealthCheck` resource. This resource defines a template for how individual VMs should be checked for health, via HTTPS.

**Note:** `google_compute_https_health_check` is a legacy health check. The newer `google_compute_health_check` should be preferred for all uses except Network Load Balancers which still require the legacy version.

To get more information about `HttpsHealthCheck`, see:

- API documentation
- How-to Guides
  - Adding Health Checks



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Https Health Check Basic

```
resource "google_compute_https_health_check" "default" {
  name          = "authentication-health-check"
  request_path  = "/health_check"

  timeout_sec      = 1
  check_interval_sec = 1
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which

means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

- 
- **check\_interval\_sec** - (Optional) How often (in seconds) to send a health check. The default value is 5 seconds.
  - **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.
  - **healthy\_threshold** - (Optional) A so-far unhealthy instance will be marked healthy after this many consecutive successes. The default value is 2.
  - **host** - (Optional) The value of the host header in the HTTPS health check request. If left empty (default value), the public IP on behalf of which this health check is performed will be used.
  - **port** - (Optional) The TCP port number for the HTTPS health check request. The default value is 80.
  - **request\_path** - (Optional) The request path of the HTTPS health check request. The default value is /.
  - **timeout\_sec** - (Optional) How long (in seconds) to wait before claiming failure. The default value is 5 seconds. It is invalid for timeoutSec to have greater value than checkIntervalSec.
  - **unhealthy\_threshold** - (Optional) A so-far healthy instance will be marked unhealthy after this many consecutive failures. The default value is 2.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.



- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

HttpsHealthCheck can be imported using any of these accepted formats:

```
$ terraform import google_compute_https_health_check.default projects/{{project}}/global/httpsHealthCheck/{{name}}
$ terraform import google_compute_https_health_check.default {{project}}/{{name}}
$ terraform import google_compute_https_health_check.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_compute_image`

Represents an Image resource.

Google Compute Engine uses operating system images to create the root persistent disks for your instances. You specify an image when you create an instance. Images contain a boot loader, an operating system, and a root file system. Linux operating system images are also capable of running containers on Compute Engine.

Images can be either public or custom.

Public images are provided and maintained by Google, open-source communities, and third-party vendors. By default, all projects have access to these images and can use them to create instances. Custom images are available only to your project. You can create a custom image from root persistent disks and other images. Then, use the custom image to create an instance.

To get more information about Image, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Image Basic

```
resource "google_compute_image" "example" {  
  name = "example-image"  
  
  raw_disk {  
    source = "https://storage.googleapis.com/bosh-cpi-artifacts/bosh-stemcell-3262.4-google-  
  }  
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource; provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- 
- **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.
  - **disk\_size\_gb** - (Optional) Size of the image when restored onto a persistent disk (in GB).
  - **family** - (Optional) The name of the image family to which this image belongs. You can create disks by specifying an image family instead of a specific image name. The image family always returns its latest image that is not deprecated. The name of the image family must comply with RFC1035.
  - **labels** - (Optional) Labels to apply to this Image.
  - **licenses** - (Optional) Any applicable license URI.
  - **raw\_disk** - (Optional) The parameters of the raw disk image. Structure is documented below.
  - **source\_disk** - (Optional) The source disk to create this image based on. You must provide either this property or the `rawDisk.source` property but not both to create an image.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The `raw_disk` block supports:

- `container_type` - (Optional) The format used to encode and transmit the block device, which should be TAR. This is just a container and transmission format and not a runtime format. Provided by the client when the disk image is created.
- `sha1` - (Optional) An optional SHA1 checksum of the disk image before unpackaging. This is provided by the client when the disk image is created.
- `source` - (Required) The full Google Cloud Storage URL where disk storage is stored. You must provide either this property or the `sourceDisk` property but not both.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `archive_size_bytes` - Size of the image tar.gz archive stored in Google Cloud Storage (in bytes).
- `creation_timestamp` - Creation timestamp in RFC3339 text format.
- `label_fingerprint` - The fingerprint used for optimistic locking of this resource. Used internally during updates.
- `self_link` - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Image can be imported using any of these accepted formats:

```
$ terraform import google_compute_image.default projects/{{project}}/global/images/{{name}}
$ terraform import google_compute_image.default {{project}}/{{name}}
$ terraform import google_compute_image.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_compute\_\_instance

Manages a VM instance resource within GCE. For more information see the official documentation and API.

### » Example Usage

```
resource "google_compute_instance" "default" {
  name          = "test"
  machine_type  = "n1-standard-1"
  zone          = "us-central1-a"

  tags = ["foo", "bar"]

  boot_disk {
    initialize_params {
      image = "debian-cloud/debian-9"
    }
  }

  // Local SSD disk
  scratch_disk {
  }

  network_interface {
    network = "default"

    access_config {
      // Ephemeral IP
    }
  }

  metadata = {
    foo = "bar"
  }

  metadata_startup_script = "echo hi > /test.txt"

  service_account {
    scopes = ["userinfo-email", "compute-ro", "storage-ro"]
  }
}
```

## » Argument Reference

The following arguments are supported:

- **boot\_disk** - (Required) The boot disk for the instance. Structure is documented below.
- **machine\_type** - (Required) The machine type to create.

**Note:** If you want to update this value (resize the VM) after initial creation, you must set **allow\_stopping\_for\_update** to **true**.

Custom machine types can be formatted as **custom-NUMBER\_OF\_CPUS-AMOUNT\_OF\_MEMORY\_MB**, e.g. **custom-6-20480** for 6 vCPU and 20GB of RAM.

There is a limit of 6.5 GB per CPU unless you add extended memory. You must do this explicitly by adding the suffix **-ext**, e.g. **custom-2-15360-ext** for 2 vCPU and 15 GB of memory.

- **name** - (Required) A unique name for the resource, required by GCE. Changing this forces a new resource to be created.
- **zone** - (Required) The zone that the machine should be created in.
- **network\_interface** - (Required) Networks to attach to the instance. This can be specified multiple times. Structure is documented below.

- 
- **allow\_stopping\_for\_update** - (Optional) If true, allows Terraform to stop the instance to update its properties. If you try to update a property that requires stopping the instance without setting this field, the update will fail.
  - **attached\_disk** - (Optional) Additional disks to attach to the instance. Can be repeated multiple times for multiple disks. Structure is documented below.
  - **can\_ip\_forward** - (Optional) Whether to allow sending and receiving of packets with non-matching source or destination IPs. This defaults to false.
  - **create\_timeout** - (Optional) Configurable timeout in minutes for creating instances. Default is 4 minutes. Changing this forces a new resource to be created.
  - **description** - (Optional) A brief description of this resource.
  - **deletion\_protection** - (Optional) Enable deletion protection on this instance. Defaults to false. **Note:** you must disable deletion protection before removing the resource (e.g., via **terraform destroy**), or the instance cannot be deleted and the Terraform run will not complete successfully.

- **hostname** - (Optional) A custom hostname for the instance. Must be a fully qualified DNS name and RFC-1035-valid. Valid format is a series of labels 1-63 characters long matching the regular expression `[a-z]([-a-z0-9]*[a-z0-9])`, concatenated with periods. The entire hostname must not exceed 253 characters. Changing this forces a new resource to be created.
- **guest\_accelerator** - (Optional) List of the type and count of accelerator cards attached to the instance. Structure documented below. **Note:** GPU accelerators can only be used with **on\_host\_maintenance** option set to **TERMINATE**.
- **labels** - (Optional) A set of key/value label pairs to assign to the instance.
- **metadata** - (Optional) Metadata key/value pairs to make available from within the instance. Ssh keys attached in the Cloud Console will be removed. Add them to your config in order to keep them attached to your instance.
- **metadata\_startup\_script** - (Optional) An alternative to using the `startup-script` metadata key, except this one forces the instance to be recreated (thus re-running the script) if it is changed. This replaces the `startup-script` metadata key on the created instance and thus the two mechanisms are not allowed to be used simultaneously.
- **min\_cpu\_platform** - (Optional) Specifies a minimum CPU platform for the VM instance. Applicable values are the friendly names of CPU platforms, such as **Intel Haswell** or **Intel Skylake**. See the complete list [here](#). **Note:** **allow\_stopping\_for\_update** must be set to true in order to update this field.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **scheduling** - (Optional) The scheduling strategy to use. More details about this configuration option are detailed below.
- **scratch\_disk** - (Optional) Scratch disks to attach to the instance. This can be specified multiple times for multiple scratch disks. Structure is documented below.
- **service\_account** - (Optional) Service account to attach to the instance. Structure is documented below. **Note:** **allow\_stopping\_for\_update** must be set to true in order to update this field.
- **tags** - (Optional) A list of tags to attach to the instance.

---

The `boot_disk` block supports:

- **auto\_delete** - (Optional) Whether the disk will be auto-deleted when the instance is deleted. Defaults to true.
- **device\_name** - (Optional) Name with which attached disk will be accessible. On the instance, this device will be `/dev/disk/by-id/google-{{device_name}}`.
- **disk\_encryption\_key\_raw** - (Optional) A 256-bit customer-supplied encryption key, encoded in RFC 4648 base64 to encrypt this disk.
- **initialize\_params** - (Optional) Parameters for a new disk that will be created alongside the new instance. Either **initialize\_params** or **source** must be set. Structure is documented below.
- **source** - (Optional) The name or `self_link` of the existing disk (such as those managed by `google_compute_disk`) to attach.

The **initialize\_params** block supports:

- **size** - (Optional) The size of the image in gigabytes. If not specified, it will inherit the size of its base image.
- **type** - (Optional) The GCE disk type. May be set to `pd-standard` or `pd-ssd`.
- **image** - (Optional) The image from which to initialize this disk. This can be one of: the image's `self_link`, `projects/{project}/global/images/{image}`, `projects/{project}/global/images/family/{family}`, `global/images/{image}`, `global/images/family/{family}`, `family/{family}`, `{project}/{family}`, `{project}/{image}`, `{family}`, or `{image}`. If referred by family, the images names must include the family name. If they don't, use the `google_compute_image` data source. For instance, the image `centos-6-v20180104` includes its family name `centos-6`. These images can be referred by family name here.

The **scratch\_disk** block supports:

- **interface** - (Optional) The disk interface to use for attaching this disk; either SCSI or NVME. Defaults to SCSI.

The **attached\_disk** block supports:

- **source** - (Required) The name or `self_link` of the disk to attach to this instance.
- **device\_name** - (Optional) Name with which the attached disk will be accessible under `/dev/disk/by-id/`
- **mode** - (Optional) Either `"READ_ONLY"` or `"READ_WRITE"`, defaults to `"READ_WRITE"` If you have a persistent disk with data that you want to share between multiple instances, detach it from any read-write instances and attach it to one or more instances in read-only mode.

- **disk\_encryption\_key\_raw** - (Optional) A 256-bit customer-supplied encryption key, encoded in RFC 4648 base64 to encrypt this disk.

The **network\_interface** block supports:

- **network** - (Optional) The name or **self\_link** of the network to attach this interface to. Either **network** or **subnetwork** must be provided.
- **subnetwork** - (Optional) The name or **self\_link** of the subnetwork to attach this interface to. The subnetwork must exist in the same region this instance will be created in. Either **network** or **subnetwork** must be provided.
- **subnetwork\_project** - (Optional) The project in which the subnetwork belongs. If the **subnetwork** is a **self\_link**, this field is ignored in favor of the project defined in the subnetwork **self\_link**. If the **subnetwork** is a name and this field is not provided, the provider project is used.
- **network\_ip** - (Optional) The private IP address to assign to the instance. If empty, the address will be automatically assigned.
- **access\_config** - (Optional) Access configurations, i.e. IPs via which this instance can be accessed via the Internet. Omit to ensure that the instance is not accessible from the Internet. If omitted, ssh provisioners will not work unless Terraform can send traffic to the instance's network (e.g. via tunnel or because it is running on another cloud instance on that network). This block can be repeated multiple times. Structure documented below.
- **alias\_ip\_range** - (Optional) An array of alias IP ranges for this network interface. Can only be specified for network interfaces on subnet-mode networks. Structure documented below.

The **access\_config** block supports:

- **nat\_ip** - (Optional) The IP address that will be 1:1 mapped to the instance's network ip. If not given, one will be generated.
- **public\_ptr\_domain\_name** - (Optional) The DNS domain name for the public PTR record. To set this field on an instance, you must be verified as the owner of the domain. See the docs for how to become verified as a domain owner.
- **network\_tier** - (Optional) The networking tier used for configuring this instance. This field can take the following values: PREMIUM or STANDARD. If this field is not specified, it is assumed to be PREMIUM.

The **alias\_ip\_range** block supports:

- **ip\_cidr\_range** - The IP CIDR range represented by this alias IP range. This IP CIDR range must belong to the specified subnetwork and cannot contain IP addresses reserved by system or used by other network inter-



faces. This range may be a single IP address (e.g. 10.2.3.4), a netmask (e.g. /24) or a CIDR format string (e.g. 10.1.2.0/24).

- **subnetwork\_range\_name** - (Optional) The subnetwork secondary range name specifying the secondary range from which to allocate the IP CIDR range for this alias IP range. If left unspecified, the primary range of the subnetwork will be used.

The **service\_account** block supports:

- **email** - (Optional) The service account e-mail address. If not given, the default Google Compute Engine service account is used. **Note:** **allow\_stopping\_for\_update** must be set to true in order to update this field.
- **scopes** - (Required) A list of service scopes. Both OAuth2 URLs and gcloud short names are supported. To allow full access to all Cloud APIs, use the **cloud-platform** scope. See a complete list of scopes here. **Note:** **allow\_stopping\_for\_update** must be set to true in order to update this field.

The **scheduling** block supports:

- **preemptible** - (Optional) Specifies if the instance is preemptible. If this field is set to true, then **automatic\_restart** must be set to false. Defaults to false.
- **on\_host\_maintenance** - (Optional) Describes maintenance behavior for the instance. Can be MIGRATE or TERMINATE, for more info, read [here](#).
- **automatic\_restart** - (Optional) Specifies if the instance should be restarted if it was terminated by Compute Engine (not a user). Defaults to true.

The **guest\_accelerator** block supports:

- **type** (Required) - The accelerator type resource to expose to this instance. E.g. **nvidia-tesla-k80**.
- **count** (Required) - The number of the guest accelerator cards exposed to this instance.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **instance\_id** - The server-assigned unique identifier of this instance.
- **metadata\_fingerprint** - The unique fingerprint of the metadata.

- `self_link` - The URI of the created resource.
- `tags_fingerprint` - The unique fingerprint of the tags.
- `label_fingerprint` - The unique fingerprint of the labels.
- `cpu_platform` - The CPU platform used by this instance.
- `network_interface.0.network_ip` - The internal ip address of the instance, either manually or dynamically assigned.
- `network_interface.0.access_config.0.nat_ip` - If the instance has an access config, either the given external ip (in the `nat_ip` field) or the ephemeral (generated) ip (if you didn't provide one).
- `attached_disk.0.disk_encryption_key_sha256` - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.
- `boot_disk.disk_encryption_key_sha256` - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.
- `disk.0.disk_encryption_key_sha256` - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.

## » Import

**Note:** The fields `boot_disk.0.disk_encryption_raw` and `attached_disk.*.disk_encryption_key_raw` cannot be imported automatically. The API doesn't return this information. If you are setting one of these fields in your config, you will need to update your state manually after importing the resource.

Instances can be imported using the `project`, `zone` and `name`, e.g.

```
$ terraform import google_compute_instance.default gcp-project/us-central1-a/test
```

## » `google__compute__instance__from__template`

Manages a VM instance resource within GCE. For more information see the official documentation and API.

This resource is specifically to create a compute instance from a given `source_instance_template`. To create an instance without a template, use the `google_compute_instance` resource.

## » Example Usage

```
resource "google_compute_instance_template" "tpl" {
  name = "template"
  machine_type = "n1-standard-1"

  disk {
    source_image = "debian-cloud/debian-9"
    auto_delete = true
    disk_size_gb = 100
    boot = true
  }

  network_interface {
    network = "default"
  }

  metadata = {
    foo = "bar"
  }

  can_ip_forward = true
}

resource "google_compute_instance_from_template" "tpl" {
  name          = "instance-from-template"
  zone          = "us-central1-a"

  source_instance_template = "${google_compute_instance_template.tpl.self_link}"

  // Override fields from instance template
  can_ip_forward = false
  labels = {
    my_key      = "my_value"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique name for the resource, required by GCE. Changing this forces a new resource to be created.
- **source\_instance\_template** - (Required) Name or self link of an instance template to create the instance based on.

- 
- **zone** - (Optional) The zone that the machine should be created in. If not set, the provider zone is used.

In addition to these, all arguments from `google_compute_instance` are supported as a way to override the properties in the template. All exported attributes from `google_compute_instance` are likewise exported here.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 6 minutes.
- **update** - Default is 6 minutes.
- **delete** - Default is 6 minutes.

## » google\_compute\_instance\_group

Creates a group of dissimilar Compute Engine virtual machine instances. For more information, see the official documentation and API

Recreating an instance group that's in use by another resource will give a `resourceInUseByAnotherResource` error. You can avoid this error with a Terraform `lifecycle` block as outlined in the example below.

### » Example Usage - Empty instance group

```
resource "google_compute_instance_group" "test" {
  name          = "terraform-test"
  description   = "Terraform test instance group"
  zone          = "us-central1-a"
  network       = "${google_compute_network.default.self_link}"
}
```

### » Example Usage - With instances and named ports

```
resource "google_compute_instance_group" "webservers" {
  name          = "terraform-webservers"
  description   = "Terraform test instance group"

  instances = [
    "${google_compute_instance.test.self_link}",
    "${google_compute_instance.test2.self_link}",
  ]
}
```

```

]

named_port {
  name = "http"
  port = "8080"
}

named_port {
  name = "https"
  port = "8443"
}

zone = "us-central1-a"
}

```

#### » Example Usage - Recreating an instance group in use

Recreating an instance group that's in use by another resource will give a `resourceInUseByAnotherResource` error. Use `lifecycle.create_before_destroy` as shown in this example to avoid this type of error.

```

resource "google_compute_instance_group" "staging_group" {
  name = "staging-instance-group"
  zone = "us-central1-c"
  instances = [ "${google_compute_instance.staging_vm.self_link}" ]
  named_port {
    name = "http"
    port = "8080"
  }

  named_port {
    name = "https"
    port = "8443"
  }

  lifecycle {
    create_before_destroy = true
  }
}

data "google_compute_image" "debian_image" {
  family = "debian-9"
  project = "debian-cloud"
}

```

```

resource "google_compute_instance" "staging_vm" {
  name = "staging-vm"
  machine_type = "n1-standard-1"
  zone = "us-central1-c"
  boot_disk {
    initialize_params {
      image = "${data.google_compute_image.debian_image.self_link}"
    }
  }

  network_interface {
    network = "default"
  }
}

resource "google_compute_backend_service" "staging_service" {
  name      = "staging-service"
  port_name = "https"
  protocol  = "HTTPS"

  backend {
    group = "${google_compute_instance_group.staging_group.self_link}"
  }

  health_checks = [
    "${google_compute_https_health_check.staging_health.self_link}",
  ]
}

resource "google_compute_https_health_check" "staging_health" {
  name      = "staging-health"
  request_path = "/health_check"
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the instance group. Must be 1-63 characters long and comply with RFC1035. Supported characters include lower-case letters, numbers, and hyphens.
- **zone** - (Required) The zone that this instance group should be created in.

- **description** - (Optional) An optional textual description of the instance group.
- **instances** - (Optional) List of instances in the group. They should be given as `self_link` URLs. When adding instances they must all be in the same network and zone as the instance group.
- **named\_port** - (Optional) The named port configuration. See the section below for details on configuration.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **network** - (Optional) The URL of the network the instance group is in. If this is different from the network where the instances are in, the creation fails. Defaults to the network where the instances are in (if neither **network** nor **instances** is specified, this field will be blank).

The `named_port` block supports:

- **name** - (Required) The name which the port will be mapped to.
- **port** - (Required) The port number to map the name to.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **self\_link** - The URI of the created resource.
- **size** - The number of instances in the group.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 6 minutes
- **update** - Default is 6 minutes
- **delete** - Default is 6 minutes

## » Import

Instance group can be imported using the `zone` and `name`, e.g.

```
$ terraform import google_compute_instance_group.webservers us-central1-a/terraform-webserve
```

## » google\_\_compute\_\_instance\_\_group\_\_manager

The Google Compute Engine Instance Group Manager API creates and manages pools of homogeneous Compute Engine virtual machine instances from a common instance template. For more information, see the official documentation and API

**Note:** Use google\_\_compute\_\_region\_\_instance\_\_group\_\_manager to create a regional (multi-zone) instance group manager.

### » Example Usage with top level instance template (google provider)

```
resource "google_compute_health_check" "autohealing" {
  name                = "autohealing-health-check"
  check_interval_sec  = 5
  timeout_sec         = 5
  healthy_threshold    = 2
  unhealthy_threshold = 10                                # 50 seconds

  http_health_check {
    request_path = "/healthz"
    port         = "8080"
  }
}

resource "google_compute_instance_group_manager" "appserver" {
  name = "appserver-igm"

  base_instance_name = "app"
  instance_template   = "${google_compute_instance_template.appserver.self_link}"
  update_strategy      = "NONE"
  zone                 = "us-central1-a"

  target_pools = ["${google_compute_target_pool.appserver.self_link}"]
  target_size  = 2

  named_port {
    name = "customHTTP"
    port = 8888
  }

  auto_healing_policies {
    health_check          = "${google_compute_health_check.autohealing.self_link}"
    initial_delay_sec     = 300
  }
}
```



```

    }
}

```

## » Example Usage with multiple versions (google-beta provider)

```

resource "google_compute_instance_group_manager" "appserver" {
  name = "appserver-igm"

  base_instance_name = "app"
  update_strategy    = "NONE"
  zone               = "us-central1-a"

  target_size = 5

  version {
    instance_template = "${google_compute_instance_template.appserver.self_link}"
  }

  version {
    instance_template = "${google_compute_instance_template.appserver-canary.self_link}"
    target_size {
      fixed = 1
    }
  }
}

```

## » Argument Reference

The following arguments are supported:

- **base\_instance\_name** - (Required) The base instance name to use for instances in this group. The value must be a valid RFC1035 name. Supported characters are lowercase letters, numbers, and hyphens (-). Instances are named by appending a hyphen and a random four-character string to the base instance name.
- **instance\_template** - (Required, GA) The full URL to an instance template from which all new instances will be created. This field is only present in the **google** provider.
- **version** - (Required, Beta) Application versions managed by this instance group. Each version deals with a specific instance template, allowing canary release scenarios. Structure is documented below.

- **name** - (Required) The name of the instance group manager. Must be 1-63 characters long and comply with RFC1035. Supported characters include lowercase letters, numbers, and hyphens.
- **zone** - (Required) The zone that instances in this group should be created in.

- 
- **description** - (Optional) An optional textual description of the instance group manager.
  - **named\_port** - (Optional) The named port configuration. See the section below for details on configuration.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
  - **update\_strategy** - (Optional, Default "REPLACE") If the `instance_template` resource is modified, a value of "NONE" will prevent any of the managed instances from being restarted by Terraform. A value of "REPLACE" will restart all of the instances at once. This field is only present in the `google` provider.
  - **target\_size** - (Optional) The target number of running instances for this managed instance group. This value should always be explicitly set unless this resource is attached to an autoscaler, in which case it should never be set. Defaults to 0.
  - **target\_pools** - (Optional) The full URL of all target pools to which new instances in the group are added. Updating the target pools attribute does not affect existing instances.
  - **wait\_for\_instances** - (Optional) Whether to wait for all instances to be created/updated before returning. Note that if this is set to true and the operation does not succeed, Terraform will continue trying until it times out.

- 
- **auto\_healing\_policies** - (Optional, Beta) The autohealing policies for this managed instance group. You can specify only one value. Structure is documented below. For more information, see the official documentation.
  - **update\_policy** - (Optional, Beta) The update policy for this managed instance group. Structure is documented below. For more information, see the official documentation and API

---

The `update_policy` block supports:

```
update_policy{
```

```

    type = "PROACTIVE"
    minimal_action = "REPLACE"
    max_surge_percent = 20
    max_unavailable_fixed = 2
    min_ready_sec = 50
}

```

- **minimal\_action** - (Required) - Minimal action to be taken on an instance. Valid values are "RESTART", "REPLACE"
- **type** - (Required) - The type of update. Valid values are "OPPORTUNISTIC", "PROACTIVE"
- **max\_surge\_fixed** - (Optional), The maximum number of instances that can be created above the specified `targetSize` during the update process. Conflicts with **max\_surge\_percent**. If neither is set, defaults to 1
- **max\_surge\_percent** - (Optional), The maximum number of instances(calculated as percentage) that can be created above the specified `targetSize` during the update process. Conflicts with **max\_surge\_fixed**.
- **max\_unavailable\_fixed** - (Optional), The maximum number of instances that can be unavailable during the update process. Conflicts with **max\_unavailable\_percent**. If neither is set, defaults to 1
- **max\_unavailable\_percent** - (Optional), The maximum number of instances(calculated as percentage) that can be unavailable during the update process. Conflicts with **max\_unavailable\_fixed**.
- **min\_ready\_sec** - (Optional), Minimum number of seconds to wait for after a newly created instance becomes available. This value must be from range [0, 3600]

---

The **named\_port** block supports: (Include a **named\_port** block for each named-port required).

- **name** - (Required) The name of the port.
- **port** - (Required) The port number.

---

The **auto\_healing\_policies** block supports:

- **health\_check** - (Required) The health check resource that signals auto-healing.
- **initial\_delay\_sec** - (Required) The number of seconds that the managed instance group waits before it applies autohealing policies to new instances or recently recreated instances. Between 0 and 3600.

The **version** block supports:

```

version {
  name = "appserver-canary"
  instance_template = "${google_compute_instance_template.appserver-canary.self_link}"
  target_size {
    fixed = 1
  }
}

version {
  name = "appserver-canary"
  instance_template = "${google_compute_instance_template.appserver-canary.self_link}"
  target_size {
    percent = 20
  }
}

```

- **name** - (Required) - Version name.
- **instance\_template** - (Required) - The full URL to an instance template from which all new instances of this version will be created.
- **target\_size** - (Optional) - The number of instances calculated as a fixed number or a percentage depending on the settings. Structure is documented below.

Exactly one **version** you specify must not have a **target\_size** specified. During a rolling update, the instance group manager will fulfill the **target\_size** constraints of every other **version**, and any remaining instances will be provisioned with the version where **target\_size** is unset.

The **target\_size** block supports:

- **fixed** - (Optional), The number of instances which are managed for this version. Conflicts with **percent**.
- **percent** - (Optional), The number of instances (calculated as percentage) which are managed for this version. Conflicts with **fixed**. Note that when using **percent**, rounding will be in favor of explicitly set **target\_size** values; a managed instance group with 2 instances and 2 **versions**, one of which has a **target\_size.percent** of 60 will create 2 instances of that **version**.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **fingerprint** - The fingerprint of the instance group manager.

- `instance_group` - The full URL of the instance group created by the manager.
- `self_link` - The URL of the created resource.

## » Import

Instance group managers can be imported using the `name`, e.g.

```
$ terraform import google_compute_instance_group_manager.appserver appserver-igm
```

## » `google_compute_instance_template`

Manages a VM instance template resource within GCE. For more information see the official documentation and API.

## » Example Usage

```
resource "google_compute_instance_template" "default" {
  name          = "appserver-template"
  description   = "This template is used to create app server instances."

  tags = ["foo", "bar"]

  labels = {
    environment = "dev"
  }

  instance_description = "description assigned to instances"
  machine_type         = "n1-standard-1"
  can_ip_forward       = false

  scheduling {
    automatic_restart    = true
    on_host_maintenance = "MIGRATE"
  }

  // Create a new boot disk from an image
  disk {
    source_image = "debian-cloud/debian-9"
    auto_delete = true
    boot        = true
  }
}
```

```

// Use an existing disk resource
disk {
  // Instance Templates reference disks by name, not self link
  source      = "${google_compute_disk.foobar.name}"
  auto_delete = false
  boot        = false
}

network_interface {
  network = "default"
}

metadata = {
  foo = "bar"
}

service_account {
  scopes = ["userinfo-email", "compute-ro", "storage-ro"]
}
}

data "google_compute_image" "my_image" {
  family  = "debian-9"
  project = "debian-cloud"
}

resource "google_compute_disk" "foobar" {
  name  = "existing-disk"
  image = "${data.google_compute_image.my_image.self_link}"
  size  = 10
  type  = "pd-ssd"
  zone  = "us-central1-a"
}

```

## » Using with Instance Group Manager

Instance Templates cannot be updated after creation with the Google Cloud Platform API. In order to update an Instance Template, Terraform will destroy the existing resource and create a replacement. In order to effectively use an Instance Template resource with an Instance Group Manager resource, it's recommended to specify `create_before_destroy` in a lifecycle block. Either omit the Instance Template `name` attribute, or specify a partial name with `name_prefix`. Example:

```

resource "google_compute_instance_template" "instance_template" {
  name_prefix = "instance-template-"
  machine_type = "n1-standard-1"
  region      = "us-central1"

  // boot disk
  disk {
    # ...
  }

  // networking
  network_interface {
    # ...
  }

  lifecycle {
    create_before_destroy = true
  }
}

resource "google_compute_instance_group_manager" "instance_group_manager" {
  name                = "instance-group-manager"
  instance_template   = "${google_compute_instance_template.instance_template.self_link}"
  base_instance_name = "instance-group-manager"
  zone                = "us-central1-f"
  target_size         = "1"
}

```

With this setup Terraform generates a unique name for your Instance Template and can then update the Instance Group manager without conflict before destroying the previous Instance Template.

## » Deploying the Latest Image

A common way to use instance templates and managed instance groups is to deploy the latest image in a family, usually the latest build of your application. There are two ways to do this in Terraform, and they have their pros and cons. The difference ends up being in how "latest" is interpreted. You can either deploy the latest image available when Terraform runs, or you can have each instance check what the latest image is when it's being created, either as part of a scaling event or being rebuilt by the instance group manager.

If you're not sure, we recommend deploying the latest image available when Terraform runs, because this means all the instances in your group will be based on the same image, always, and means that no upgrades or changes to your instances happen outside of a `terraform apply`. You can achieve this

by using the `google_compute_image` data source, which will retrieve the latest image on every `terraform apply`, and will update the template to use that specific image:

```
data "google_compute_image" "my_image" {
  family  = "debian-9"
  project = "debian-cloud"
}

resource "google_compute_instance_template" "instance_template" {
  name_prefix = "instance-template-"
  machine_type = "n1-standard-1"
  region      = "us-central1"

  // boot disk
  disk {
    initialize_params {
      image = "${data.google_compute_image.my_image.self_link}"
    }
  }
}
```

To have instances update to the latest on every scaling event or instance re-creation, use the family as the image for the disk, and it will use GCP's default behavior, setting the image for the template to the family:

```
resource "google_compute_instance_template" "instance_template" {
  name_prefix = "instance-template-"
  machine_type = "n1-standard-1"
  region      = "us-central1"

  // boot disk
  disk {
    initialize_params {
      image = "debian-cloud/debian-9"
    }
  }
}
```

## » Argument Reference

Note that changing any field for this resource forces a new resource to be created.

The following arguments are supported:

- `disk` - (Required) Disks to attach to instances created from this template.



This can be specified multiple times for multiple disks. Structure is documented below.

- **machine\_type** - (Required) The machine type to create.

**Note:** If you want to update this value (resize the VM) after initial creation, you must set **allow\_stopping\_for\_update** to **true**.

To create a machine with a custom type (such as extended memory), format the value like **custom-VCPUS-MEM\_IN\_MB** like **custom-6-20480** for 6 vCPU and 20GB of RAM.

- 
- **name** - (Optional) The name of the instance template. If you leave this blank, Terraform will auto-generate a unique name.
  - **name\_prefix** - (Optional) Creates a unique name beginning with the specified prefix. Conflicts with **name**.
  - **can\_ip\_forward** - (Optional) Whether to allow sending and receiving of packets with non-matching source or destination IPs. This defaults to **false**.
  - **description** - (Optional) A brief description of this resource.
  - **instance\_description** - (Optional) A brief description to use for instances created from this template.
  - **labels** - (Optional) A set of key/value label pairs to assign to instances created from this template,
  - **metadata** - (Optional) Metadata key/value pairs to make available from within instances created from this template.
  - **metadata\_startup\_script** - (Optional) An alternative to using the **startup-script** metadata key, mostly to match the **compute\_instance** resource. This replaces the **startup-script** metadata key on the created instance and thus the two mechanisms are not allowed to be used simultaneously.
  - **network\_interface** - (Required) Networks to attach to instances created from this template. This can be specified multiple times for multiple networks. Structure is documented below.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
  - **region** - (Optional) An instance template is a global resource that is not bound to a zone or a region. However, you can still specify some regional resources in an instance template, which restricts the template to the region where that resource resides. For example, a custom **subnetwork**

resource is tied to a specific region. Defaults to the region of the Provider if no value is given.

- **scheduling** - (Optional) The scheduling strategy to use. More details about this configuration option are detailed below.
- **service\_account** - (Optional) Service account to attach to the instance. Structure is documented below.
- **tags** - (Optional) Tags to attach to the instance.
- **guest\_accelerator** - (Optional) List of the type and count of accelerator cards attached to the instance. Structure documented below.
- **min\_cpu\_platform** - (Optional) Specifies a minimum CPU platform. Applicable values are the friendly names of CPU platforms, such as **Intel Haswell** or **Intel Skylake**. See the complete list [here](#).

The **disk** block supports:

- **auto\_delete** - (Optional) Whether or not the disk should be auto-deleted. This defaults to true.
- **boot** - (Optional) Indicates that this is a boot disk.
- **device\_name** - (Optional) A unique device name that is reflected into the `/dev/` tree of a Linux operating system running within the instance. If not specified, the server chooses a default device name to apply to this disk.
- **disk\_name** - (Optional) Name of the disk. When not provided, this defaults to the name of the instance.
- **source\_image** - (Required if source not set) The image from which to initialize this disk. This can be one of: the image's **self\_link**, `projects/{project}/global/images/{image}`, `projects/{project}/global/images/family/{family}`, `global/images/{image}`, `global/images/family/{family}`, `family/{family}`, `{project}/{family}`, `{project}/{image}`, `{family}`, or `{image}`.
- **interface** - (Optional) Specifies the disk interface to use for attaching this disk.
- **mode** - (Optional) The mode in which to attach this disk, either `READ_WRITE` or `READ_ONLY`. If you are attaching or creating a boot disk, this must read-write mode.
- **source** - (Required if **source\_image** not set) The name (**not **self\_link****) of the disk (such as those managed by `google_compute_disk`) to attach.
- **disk\_type** - (Optional) The GCE disk type. Can be either `"pd-ssd"`, `"local-ssd"`, or `"pd-standard"`.
- **disk\_size\_gb** - (Optional) The size of the image in gigabytes. If not specified, it will inherit the size of its base image.

- **type** - (Optional) The type of GCE disk, can be either "SCRATCH" or "PERSISTENT".
- **disk\_encryption\_key** - (Optional) Encrypts or decrypts a disk using a customer-supplied encryption key.

If you are creating a new disk, this field encrypts the new disk using an encryption key that you provide. If you are attaching an existing disk that is already encrypted, this field decrypts the disk using the customer-supplied encryption key.

If you encrypt a disk using a customer-supplied key, you must provide the same key again when you attempt to use this resource at a later time. For example, you must provide the key when you create a snapshot or an image from the disk or when you attach the disk to a virtual machine instance.

If you do not provide an encryption key, then the disk will be encrypted using an automatically generated key and you do not need to provide a key to use the disk later.

Instance templates do not store customer-supplied encryption keys, so you cannot use your own keys to encrypt disks in a managed instance group.

The **disk\_encryption\_key** block supports:

- **kms\_key\_self\_link** - (Optional) The self link of the encryption key that is stored in Google Cloud KMS

The **network\_interface** block supports:

- **network** - (Optional) The name or self\_link of the network to attach this interface to. Use **network** attribute for Legacy or Auto subnetted networks and **subnetwork** for custom subnetted networks.
- **subnetwork** - (Optional) the name of the subnetwork to attach this interface to. The subnetwork must exist in the same **region** this instance will be created in. Either **network** or **subnetwork** must be provided.
- **subnetwork\_project** - (Optional) The ID of the project in which the subnetwork belongs. If it is not provided, the provider project is used.
- **network\_ip** - (Optional) The private IP address to assign to the instance. If empty, the address will be automatically assigned.
- **access\_config** - (Optional) Access configurations, i.e. IPs via which this instance can be accessed via the Internet. Omit to ensure that the instance is not accessible from the Internet (this means that ssh provisioners will not work unless you are running Terraform can send traffic to the instance's network (e.g. via tunnel or because it is running on another cloud instance on that network). This block can be repeated multiple times. Structure documented below.

- **alias\_ip\_range** - (Optional) An array of alias IP ranges for this network interface. Can only be specified for network interfaces on subnet-mode networks. Structure documented below.

The **access\_config** block supports:

- **nat\_ip** - (Optional) The IP address that will be 1:1 mapped to the instance's network ip. If not given, one will be generated.
- **network\_tier** - (Optional) The networking tier used for configuring this instance template. This field can take the following values: PREMIUM or STANDARD. If this field is not specified, it is assumed to be PREMIUM.

The **alias\_ip\_range** block supports:

- **ip\_cidr\_range** - The IP CIDR range represented by this alias IP range. This IP CIDR range must belong to the specified subnetwork and cannot contain IP addresses reserved by system or used by other network interfaces. At the time of writing only a netmask (e.g. /24) may be supplied, with a CIDR format resulting in an API error.
- **subnetwork\_range\_name** - (Optional) The subnetwork secondary range name specifying the secondary range from which to allocate the IP CIDR range for this alias IP range. If left unspecified, the primary range of the subnetwork will be used.

The **service\_account** block supports:

- **email** - (Optional) The service account e-mail address. If not given, the default Google Compute Engine service account is used.
- **scopes** - (Required) A list of service scopes. Both OAuth2 URLs and gcloud short names are supported. To allow full access to all Cloud APIs, use the **cloud-platform** scope. See a complete list of scopes [here](#).

The service accounts documentation explains that access scopes are the legacy method of specifying permissions for your instance. If you are following best practices and using IAM roles to grant permissions to service accounts, then you can define this field as an empty list.

The **scheduling** block supports:

- **automatic\_restart** - (Optional) Specifies whether the instance should be automatically restarted if it is terminated by Compute Engine (not terminated by a user). This defaults to true.
- **on\_host\_maintenance** - (Optional) Defines the maintenance behavior for this instance.
- **preemptible** - (Optional) Allows instance to be preempted. This defaults to false. Read more on this [here](#).

The **guest\_accelerator** block supports:

- **type** (Required) - The accelerator type resource to expose to this instance. E.g. `nvidia-tesla-k80`.
- **count** (Required) - The number of the guest accelerator cards exposed to this instance.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **metadata\_fingerprint** - The unique fingerprint of the metadata.
- **self\_link** - The URI of the created resource.
- **tags\_fingerprint** - The unique fingerprint of the tags.

## » Import

Instance templates can be imported using the **name**, e.g.

```
$ terraform import google_compute_instance_template.default appserver-template
```

## » google\_compute\_interconnect\_attachment

Represents an InterconnectAttachment (VLAN attachment) resource. For more information, see [Creating VLAN Attachments](#).

## » Example Usage - Interconnect Attachment Basic

```
resource "google_compute_interconnect_attachment" "on_prem" {
  name          = "on-prem-attachment"
  interconnect  = "my-interconnect-id"
  router        = "${google_compute_router.foobar.self_link}"
}

resource "google_compute_router" "foobar" {
  name    = "router"
  network = "${google_compute_network.foobar.name}"
}
```

## » Argument Reference

The following arguments are supported:

- **router** - (Required) URL of the cloud router to be used for dynamic routing. This router must be in the same region as this InterconnectAttachment. The InterconnectAttachment will automatically connect the Interconnect to the network & region within which the Cloud Router is configured.
  - **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- 
- **interconnect** - (Optional) URL of the underlying Interconnect object that this attachment's traffic will traverse through. Required if type is DEDICATED, must not be set if type is PARTNER.
  - **description** - (Optional) An optional description of this resource.
  - **edge\_availability\_domain** - (Optional) Desired availability domain for the attachment. Only available for type PARTNER, at creation time. For improved reliability, customers should configure a pair of attachments with one per availability domain. The selected availability domain will be provided to the Partner via the pairing key so that the provisioned circuit will lie in the specified domain. If not specified, the value will default to AVAILABILITY\_DOMAIN\_ANY.
  - **type** - (Optional) The type of InterconnectAttachment you wish to create. Defaults to DEDICATED.
  - **candidate\_subnets** - (Optional) Up to 16 candidate prefixes that can be used to restrict the allocation of cloudRouterIpAddress and customerRouterIpAddress for this attachment. All prefixes must be within link-local address space (169.254.0.0/16) and must be /29 or shorter (/28, /27, etc). Google will attempt to select an unused /29 from the supplied candidate prefix(es). The request will fail if all possible /29s are in use on Google's edge. If not supplied, Google will randomly select an unused /29 from all of link-local space.
  - **vlan\_tag8021q** - (Optional) The IEEE 802.1Q VLAN tag for this attachment, in the range 2-4094.

- **region** - (Optional) Region where the regional interconnect attachment resides.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **cloud\_router\_ip\_address** - IPv4 address + prefix length to be configured on Cloud Router Interface for this interconnect attachment.
- **customer\_router\_ip\_address** - IPv4 address + prefix length to be configured on the customer router subinterface for this interconnect attachment.
- **pairing\_key** - [Output only for type PARTNER. Not present for DEDICATED]. The opaque identifier of an PARTNER attachment used to initiate provisioning with a selected partner. Of the form "XXXXX/region/domain"
- **partner\_asn** - [Output only for type PARTNER. Not present for DEDICATED]. Optional BGP ASN for the router that should be supplied by a layer 3 Partner if they configured BGP on behalf of the customer.
- **private\_interconnect\_info** - Information specific to an InterconnectAttachment. This property is populated if the interconnect that this is attached to is of type DEDICATED. Structure is documented below.
- **state** - [Output Only] The current state of this attachment's functionality.
- **google\_reference\_id** - Google reference ID, to be used when raising support tickets with Google or otherwise to debug backend connectivity issues.
- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **self\_link** - The URI of the created resource.

The **private\_interconnect\_info** block contains:

- **tag8021q** - 802.1q encapsulation tag to be used for traffic between Google and the customer, going to and from this network and region.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.

- `delete` - Default is 4 minutes.

## » Import

InterconnectAttachment can be imported using any of these accepted formats:

```
$ terraform import google_compute_interconnect_attachment.default projects/{{project}}/regions/{{region}}/interconnectAttachments/{{name}}
$ terraform import google_compute_interconnect_attachment.default {{project}}/{{region}}/{{name}}
$ terraform import google_compute_interconnect_attachment.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_compute_network`

Manages a VPC network or legacy network resource on GCP.

To get more information about Network, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Network Basic

```
resource "google_compute_network" "vpc_network" {
  name = "vpc-network"
}
```

## » Argument Reference

The following arguments are supported:

- `name` - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which



means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

- 
- **description** - (Optional) An optional description of this resource. The resource must be recreated to modify this field.
  - **ipv4\_range** - (Optional, Deprecated) If this field is specified, a deprecated legacy network is created. You will no longer be able to create a legacy network on Feb 1, 2020. See the legacy network docs for more details. The range of internal addresses that are legal on this legacy network. This range is a CIDR specification, for example: `192.168.0.0/16`. The resource must be recreated to modify this field.
  - **auto\_create\_subnetworks** - (Optional) When set to `true`, the network is created in "auto subnet mode" and it will create a subnet for each region automatically across the `10.128.0.0/9` address range. When set to `false`, the network is created in "custom subnet mode" so the user can explicitly connect subnetwork resources.
  - **routing\_mode** - (Optional) The network-wide routing mode to use. If set to `REGIONAL`, this network's cloud routers will only advertise routes with subnetworks of this network in the same region as the router. If set to `GLOBAL`, this network's cloud routers will advertise routes with all subnetworks of this network, across regions.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **gateway\_ipv4** - The gateway address for default routing out of the network. This value is selected by GCP.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

Network can be imported using any of these accepted formats:

```
$ terraform import google_compute_network.default projects/{{project}}/global/networks/{{name}}
$ terraform import google_compute_network.default {{project}}/{{name}}
$ terraform import google_compute_network.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_network\_peering

Manages a network peering within GCE. For more information see the official documentation and API.

**Note:** Both network must create a peering with each other for the peering to be functional.

**Note:** Subnets IP ranges across peered VPC networks cannot overlap.

## » Example Usage

```
resource "google_compute_network_peering" "peering1" {
  name = "peering1"
  network = "${google_compute_network.default.self_link}"
  peer_network = "${google_compute_network.other.self_link}"
}

resource "google_compute_network_peering" "peering2" {
  name = "peering2"
  network = "${google_compute_network.other.self_link}"
  peer_network = "${google_compute_network.default.self_link}"
}

resource "google_compute_network" "default" {
  name = "foobar"
  auto_create_subnetworks = "false"
}

resource "google_compute_network" "other" {
  name = "other"
  auto_create_subnetworks = "false"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the peering.
- **network** - (Required) Resource link of the network to add a peering to.
- **peer\_network** - (Required) Resource link of the peer network.
- **auto\_create\_routes** - (Optional) If set to **true**, the routes between the two networks will be created and managed automatically. Defaults to **true**.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **state** - State for the peering.
- **state\_details** - Details about the current state of the peering.

## » google\_compute\_project\_metadata

Authoritatively manages metadata common to all instances for a project in GCE. For more information see the official documentation and API.

**Note:** This resource manages all project-level metadata including project-level ssh keys. Keys unset in config but set on the server will be removed. If you want to manage only single key/value pairs within the project metadata rather than the entire set, then use `google_compute_project_metadata_item`.

## » Example Usage

```
resource "google_compute_project_metadata" "default" {
  metadata = {
    foo  = "bar"
    fizz = "buzz"
    "13" = "42"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **metadata** - (Required) A series of key value pairs.
- 
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » Import

This resource can be imported using the project ID:

```
terraform import google_compute_project_metadata.foo my-project-id
```

## » google\_compute\_project\_metadata\_item

Manages a single key/value pair on metadata common to all instances for a project in GCE. Using `google_compute_project_metadata_item` lets you manage a single key/value setting in Terraform rather than the entire project metadata map.

## » Example Usage

```
resource "google_compute_project_metadata_item" "default" {  
  key = "my_metadata"  
  value = "my_value"  
}
```

## » Argument Reference

The following arguments are supported:

- **key** - (Required) The metadata key to set.
  - **value** - (Required) The value to set for the given metadata key.
-

- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » Import

Project metadata items can be imported using the **key**, e.g.

```
$ terraform import google_compute_project_metadata_item.default my_metadata
```

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 5 minutes.
- **update** - Default is 5 minutes.
- **delete** - Default is 5 minutes.

## » google\_compute\_region\_autoscaler

Represents an Autoscaler resource.

Autoscalers allow you to automatically scale virtual machine instances in managed instance groups according to an autoscaling policy that you define.

To get more information about RegionAutoscaler, see:

- API documentation
- How-to Guides
  - Autoscaling Groups of Instances



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Region Autoscaler Beta

```
resource "google_compute_region_autoscaler" "foobar" {
  provider = "google-beta"
```

```

name      = "my-region-autoscaler"
region    = "us-central1"
target    = "${google_compute_region_instance_group_manager.foobar.self_link}"

autoscaling_policy {
  max_replicas    = 5
  min_replicas    = 1
  cooldown_period = 60

  cpu_utilization {
    target = 0.5
  }
}
}

resource "google_compute_instance_template" "foobar" {
  provider = "google-beta"

  name          = "my-instance-template"
  machine_type  = "n1-standard-1"
  can_ip_forward = false

  tags = ["foo", "bar"]

  disk {
    source_image = "${data.google_compute_image.debian_9.self_link}"
  }

  network_interface {
    network = "default"
  }

  metadata = {
    foo = "bar"
  }

  service_account {
    scopes = ["userinfo-email", "compute-ro", "storage-ro"]
  }
}

resource "google_compute_target_pool" "foobar" {
  provider = "google-beta"

  name = "my-target-pool"
}

```

```

}

resource "google_compute_region_instance_group_manager" "foobar" {
  provider = "google-beta"

  name      = "my-region-igm"
  region    = "us-central1"

  version {
    instance_template = "${google_compute_instance_template.foobar.self_link}"
    name              = "primary"
  }

  target_pools      = ["${google_compute_target_pool.foobar.self_link}"]
  base_instance_name = "foobar"
}

data "google_compute_image" "debian_9" {
  provider = "google-beta"

  family = "debian-9"
  project = "debian-cloud"
}

provider "google-beta" {
  region = "us-central1"
  zone   = "us-central1-a"
}

```



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Region Autoscaler Basic

```

resource "google_compute_region_autoscaler" "foobar" {
  name      = "my-region-autoscaler"
  region    = "us-central1"
  target    = "${google_compute_region_instance_group_manager.foobar.self_link}"

  autoscaling_policy {
    max_replicas    = 5
    min_replicas    = 1
    cooldown_period = 60
  }
}

```

```

        cpu_utilization {
            target = 0.5
        }
    }
}

resource "google_compute_instance_template" "foobar" {
    name          = "my-instance-template"
    machine_type  = "n1-standard-1"
    can_ip_forward = false

    tags = ["foo", "bar"]

    disk {
        source_image = "${data.google_compute_image.debian_9.self_link}"
    }

    network_interface {
        network = "default"
    }

    metadata = {
        foo = "bar"
    }

    service_account {
        scopes = ["userinfo-email", "compute-ro", "storage-ro"]
    }
}

resource "google_compute_target_pool" "foobar" {
    name = "my-target-pool"
}

resource "google_compute_region_instance_group_manager" "foobar" {
    name     = "my-region-igm"
    region  = "us-central1"

    instance_template = "${google_compute_instance_template.foobar.self_link}"

    target_pools      = ["${google_compute_target_pool.foobar.self_link}"]
    base_instance_name = "foobar"
}

data "google_compute_image" "debian_9" {

```



```

    family = "debian-9"
    project = "debian-cloud"
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. The name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- **autoscaling\_policy** - (Required) The configuration parameters for the autoscaling algorithm. You can define one or more of the policies for an autoscaler: `cpuUtilization`, `customMetricUtilizations`, and `loadBalancingUtilization`. If none of these are specified, the default will be to autoscale based on `cpuUtilization` to 0.6 or 60%. Structure is documented below.
- **target** - (Required) URL of the managed instance group that this autoscaler will scale.

The `autoscaling_policy` block supports:

- **min\_replicas** - (Required) The minimum number of replicas that the autoscaler can scale down to. This cannot be less than 0. If not provided, autoscaler will choose a default value depending on maximum number of instances allowed.
- **max\_replicas** - (Required) The maximum number of instances that the autoscaler can scale up to. This is required when creating or updating an autoscaler. The maximum number of replicas should not be lower than minimal number of replicas.
- **cooldown\_period** - (Optional) The number of seconds that the autoscaler should wait before it starts collecting information from a new instance. This prevents the autoscaler from collecting information when the instance is initializing, during which the collected usage would not be reliable. The default time autoscaler waits is 60 seconds. Virtual machine initialization times might vary because of numerous factors. We recommend that you test how long an instance may take to initialize. To do this, create an instance and time the startup process.
- **cpu\_utilization** - (Optional) Defines the CPU utilization policy that allows the autoscaler to scale based on the average CPU utilization of a managed instance group. Structure is documented below.

- **metric** - (Optional) Defines the CPU utilization policy that allows the autoscaler to scale based on the average CPU utilization of a managed instance group. Structure is documented below.
- **load\_balancing\_utilization** - (Optional) Configuration parameters of autoscaling based on a load balancer. Structure is documented below.

The **cpu\_utilization** block supports:

- **target** - (Required) The target CPU utilization that the autoscaler should maintain. Must be a float value in the range (0, 1]. If not specified, the default is 0.6. If the CPU level is below the target utilization, the autoscaler scales down the number of instances until it reaches the minimum number of instances you specified or until the average CPU of your instances reaches the target utilization. If the average CPU is above the target utilization, the autoscaler scales up until it reaches the maximum number of instances you specified or until the average utilization reaches the target utilization.

The **metric** block supports:

- **name** - (Required) The identifier (type) of the Stackdriver Monitoring metric. The metric cannot have negative values. The metric must have a value type of INT64 or DOUBLE.
- **target** - (Required) The target value of the metric that autoscaler should maintain. This must be a positive value. A utilization metric scales number of virtual machines handling requests to increase or decrease proportionally to the metric. For example, a good metric to use as a utilization-Target is [www.googleapis.com/compute/instance/network/received\\_bytes\\_count](https://www.googleapis.com/compute/instance/network/received_bytes_count). The autoscaler will work to keep this value constant for each of the instances.
- **type** - (Required) Defines how target utilization value is expressed for a Stackdriver Monitoring metric. Either GAUGE, DELTA\_PER\_SECOND, or DELTA\_PER\_MINUTE.
- **filter** - (Optional, Beta) A filter string to be used as the filter string for a Stackdriver Monitoring TimeSeries.list API call. This filter is used to select a specific TimeSeries for the purpose of autoscaling and to determine whether the metric is exporting per-instance or per-group data. You can only use the AND operator for joining selectors. You can only use direct equality comparison operator (=) without any functions for each selector. You can specify the metric in both the filter string and in the metric field. However, if specified in both places, the metric must be identical. The monitored resource type determines what kind of values are expected for the metric. If it is a gce\_instance, the autoscaler expects the metric to include a separate TimeSeries for each instance in a group. In such a case, you cannot filter on resource labels. If the resource type is any other value, the autoscaler expects this metric to contain values that apply to the entire

autoscaled instance group and resource label filtering can be performed to point autoscaler at the correct TimeSeries to scale upon. This is called a per-group metric for the purpose of autoscaling. If not specified, the type defaults to `gce_instance`. You should provide a filter that is selective enough to pick just one TimeSeries for the autoscaled group or for each of the instances (if you are using `gce_instance` resource type). If multiple TimeSeries are returned upon the query execution, the autoscaler will sum their respective values to obtain its scaling value.

The `load_balancing_utilization` block supports:

- **target** - (Required) Fraction of backend capacity utilization (set in HTTP(s) load balancing configuration) that autoscaler should maintain. Must be a positive float value. If not defined, the default is 0.8.
- 
- **description** - (Optional) An optional description of this resource.
  - **region** - (Optional) URL of the region where the instance group resides.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

RegionAutoscaler can be imported using any of these accepted formats:

```
$ terraform import google_compute_region_autoscaler.default projects/{{project}}/regions/{{region}}/{{name}}
$ terraform import google_compute_region_autoscaler.default {{region}}/{{name}}
$ terraform import google_compute_region_autoscaler.default {{project}}/{{region}}/{{name}}
$ terraform import google_compute_region_autoscaler.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_compute_region_backend_service`

A Region Backend Service defines a regionally-scoped group of virtual machines that will serve traffic for load balancing. For more information see the official documentation and API.

**Note:** Region backend services can only be used when using internal load balancing. For external load balancing, use `google_compute_backend_service` instead.

### » Example Usage

```
resource "google_compute_region_backend_service" "foobar" {
  name           = "blablah"
  description    = "Hello World 1234"
  protocol       = "TCP"
  timeout_sec    = 10
  session_affinity = "CLIENT_IP"

  backend {
    group = "${google_compute_region_instance_group_manager.foo.instance_group}"
  }

  health_checks = ["${google_compute_health_check.default.self_link}"]
}

resource "google_compute_region_instance_group_manager" "foo" {
  name           = "terraform-test"
  instance_template = "${google_compute_instance_template.foobar.self_link}"
  base_instance_name = "foobar"
  region          = "us-central1"
  target_size      = 1
}

resource "google_compute_instance_template" "foobar" {
  name           = "terraform-test"
  machine_type   = "n1-standard-1"

  network_interface {
    network = "default"
  }
}
```

```

    }

    disk {
      source_image = "debian-cloud/debian-9"
      auto_delete  = true
      boot         = true
    }
  }

  resource "google_compute_health_check" "default" {
    name                = "test"
    check_interval_sec = 1
    timeout_sec         = 1

    tcp_health_check {
      port = "80"
    }
  }
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the backend service.
  - **health\_checks** - (Required) Specifies a list of health checks for checking the health of the backend service. Currently at most one health check can be specified, and a health check is required.
- 
- **backend** - (Optional) The list of backends that serve this BackendService. Structure is documented below.
  - **description** - (Optional) The textual description for the backend service.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
  - **protocol** - (Optional) The protocol for incoming requests. Defaults to TCP.
  - **session\_affinity** - (Optional) How to distribute load. Options are NONE (no affinity), CLIENT\_IP, CLIENT\_IP\_PROTO, or CLIENT\_IP\_PORT\_PROTO. Defaults to NONE.
  - **region** - (Optional) The Region in which the created address should reside. If it is not provided, the provider region is used.

- `timeout_sec` - (Optional) The number of secs to wait for a backend to respond to a request before considering the request failed. Defaults to 30.
- `connection_draining_timeout_sec` - (Optional) Time for which instance will be drained (not accept new connections, but still work to finish started ones). Defaults to 0.

The `backend` block supports:

- `group` - (Required) The name or URI of a Compute Engine instance group (`google_compute_region_instance_group_manager.xyz.instance_group`) that can receive traffic. Instance groups must contain at least one instance.
- `description` - (Optional) Textual description for the backend.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `fingerprint` - The fingerprint of the backend service.
- `self_link` - The URI of the created resource.

## » `google_compute_region_disk`

Persistent disks are durable storage devices that function similarly to the physical disks in a desktop or a server. Compute Engine manages the hardware behind these devices to ensure data redundancy and optimize performance for you. Persistent disks are available as either standard hard disk drives (HDD) or solid-state drives (SSD).

Persistent disks are located independently from your virtual machine instances, so you can detach or move persistent disks to keep your data even after you delete your instances. Persistent disk performance scales automatically with size, so you can resize your existing persistent disks or add more persistent disks to an instance to meet your performance and storage space requirements.

Add a persistent disk to your instance when you need reliable and affordable storage with consistent performance characteristics.

To get more information about `RegionDisk`, see:

- API documentation
- How-to Guides
  - Adding or Resizing Regional Persistent Disks

**Warning:** All arguments including the disk encryption key will be stored in the raw state as plain-text. Read more about sensitive data in state.



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Region Disk Basic

```
resource "google_compute_region_disk" "regiondisk" {
  name = "my-region-disk"
  snapshot = "${google_compute_snapshot.snapdisk.self_link}"
  type = "pd-ssd"
  region = "us-central1"

  replica_zones = ["us-central1-a", "us-central1-f"]
}

resource "google_compute_disk" "disk" {
  name = "my-disk"
  image = "debian-cloud/debian-9"
  size = 50
  type = "pd-ssd"
  zone = "us-central1-a"
}

resource "google_compute_snapshot" "snapdisk" {
  name = "my-snapshot"
  source_disk = "${google_compute_disk.disk.name}"
  zone = "us-central1-a"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

- **replica\_zones** - (Required) URLs of the zones where the disk should be replicated to.

- 
- **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.

- **labels** - (Optional) Labels to apply to this disk. A list of key->value pairs.

- **size** - (Optional) Size of the persistent disk, specified in GB. You can specify this field when creating a persistent disk using the `sourceImage` or `sourceSnapshot` parameter, or specify it alone to create an empty persistent disk. If you specify this field along with `sourceImage` or `sourceSnapshot`, the value of `sizeGb` must not be less than the size of the `sourceImage` or the size of the snapshot.

- **type** - (Optional) URL of the disk type resource describing which disk type to use to create the disk. Provide this when creating the disk.

- **region** - (Optional) A reference to the region where the disk resides.

- **disk\_encryption\_key** - (Optional) Encrypts the disk using a customer-supplied encryption key. After you encrypt a disk with a customer-supplied key, you must provide the same key if you use the disk later (e.g. to create a disk snapshot or an image, or to attach the disk to a virtual machine). Customer-supplied encryption keys do not protect access to metadata of the disk. If you do not provide an encryption key when creating the disk, then the disk will be encrypted using an automatically generated key and you do not need to provide a key to use the disk later. Structure is documented below.

- **snapshot** - (Optional) The source snapshot used to create this disk. You can provide this as a partial or full URL to the resource. For example, the following are valid values:

- `https://www.googleapis.com/compute/v1/projects/project/global/snapshots/snapshot`
- `projects/project/global/snapshots/snapshot`
- `global/snapshots/snapshot`
- `snapshot`

- **source\_snapshot\_encryption\_key** - (Optional) The customer-supplied encryption key of the source snapshot. Required if the source snapshot is protected by a customer-supplied encryption key. Structure is documented below.

- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The `disk_encryption_key` block supports:



- **raw\_key** - (Optional) Specifies a 256-bit customer-supplied encryption key, encoded in RFC 4648 base64 to either encrypt or decrypt this resource.
- **sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.
- **kms\_key\_name** - (Optional, Beta) The name of the encryption key that is stored in Google Cloud KMS.

The **source\_snapshot\_encryption\_key** block supports:

- **raw\_key** - (Optional) Specifies a 256-bit customer-supplied encryption key, encoded in RFC 4648 base64 to either encrypt or decrypt this resource.
- **kms\_key\_name** - (Optional, Beta) The name of the encryption key that is stored in Google Cloud KMS.
- **sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **label\_fingerprint** - The fingerprint used for optimistic locking of this resource. Used internally during updates.
- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **last\_attach\_timestamp** - Last attach timestamp in RFC3339 text format.
- **last\_detach\_timestamp** - Last detach timestamp in RFC3339 text format.
- **users** - Links to the users of the disk (attached instances) in form: project/zones/zone/instances/instance
- **source\_snapshot\_id** - The unique ID of the snapshot used to create this disk. This value identifies the exact snapshot that was used to create this persistent disk. For example, if you created the persistent disk from a snapshot that was later deleted and recreated under the same name, the source snapshot ID would identify the exact version of the snapshot that was used.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 5 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

RegionDisk can be imported using any of these accepted formats:

```
$ terraform import google_compute_region_disk.default projects/{{project}}/regions/{{region}}/disks/{{name}}
$ terraform import google_compute_region_disk.default {{project}}/{{region}}/{{name}}
$ terraform import google_compute_region_disk.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_region\_instance\_group\_manager

The Google Compute Engine Regional Instance Group Manager API creates and manages pools of homogeneous Compute Engine virtual machine instances from a common instance template. For more information, see the official documentation and API

**Note:** Use `google_compute_instance_group_manager` to create a single-zone instance group manager.

## » Example Usage with top level instance template (google provider)

```
resource "google_compute_health_check" "autohealing" {
  name                = "autohealing-health-check"
  check_interval_sec = 5
  timeout_sec         = 5
  healthy_threshold   = 2
  unhealthy_threshold = 10                                # 50 seconds

  http_health_check {
    request_path = "/healthz"
    port         = "8080"
  }
}
```

```

}

resource "google_compute_region_instance_group_manager" "appserver" {
  name = "appserver-igm"

  base_instance_name      = "app"
  instance_template       = "${google_compute_instance_template.appserver.self_link}"
  region                  = "us-central1"
  distribution_policy_zones = ["us-central1-a", "us-central1-f"]

  target_pools = ["${google_compute_target_pool.appserver.self_link}"]
  target_size  = 2

  named_port {
    name = "custom"
    port = 8888
  }

  auto_healing_policies {
    health_check      = "${google_compute_health_check.autohealing.self_link}"
    initial_delay_sec = 300
  }
}

```

## » Example Usage with multiple versions (google-beta provider)

```

resource "google_compute_region_instance_group_manager" "appserver" {
  name = "appserver-igm"

  base_instance_name = "app"
  update_strategy     = "NONE"
  region              = "us-central1"

  target_size = 5

  version {
    instance_template = "${google_compute_instance_template.appserver.self_link}"
  }

  version {
    instance_template = "${google_compute_instance_template.appserver-canary.self_link}"
    target_size {
      fixed = 1
    }
  }
}

```

```
}  
}
```

## » Argument Reference

The following arguments are supported:

- **base\_instance\_name** - (Required) The base instance name to use for instances in this group. The value must be a valid RFC1035 name. Supported characters are lowercase letters, numbers, and hyphens (-). Instances are named by appending a hyphen and a random four-character string to the base instance name.
  - **instance\_template** - (Required, GA) The full URL to an instance template from which all new instances will be created. This field is only present in the `google` provider.
  - **version** - (Required, Beta) Application versions managed by this instance group. Each version deals with a specific instance template, allowing canary release scenarios. Structure is documented below.
  - **name** - (Required) The name of the instance group manager. Must be 1-63 characters long and comply with RFC1035. Supported characters include lowercase letters, numbers, and hyphens.
  - **region** - (Required) The region where the managed instance group resides.
- 
- **description** - (Optional) An optional textual description of the instance group manager.
  - **named\_port** - (Optional) The named port configuration. See the section below for details on configuration.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
  - **target\_size** - (Optional) The target number of running instances for this managed instance group. This value should always be explicitly set unless this resource is attached to an autoscaler, in which case it should never be set. Defaults to 0.
  - **target\_pools** - (Optional) The full URL of all target pools to which new instances in the group are added. Updating the target pools attribute does not affect existing instances.
  - **wait\_for\_instances** - (Optional) Whether to wait for all instances to be created/updated before returning. Note that if this is set to true and the operation does not succeed, Terraform will continue trying until it times out.

- 
- **auto\_healing\_policies** - (Optional, Beta) The autohealing policies for this managed instance group. You can specify only one value. Structure is documented below. For more information, see the official documentation.
  - **update\_policy** - (Optional, Beta) The update policy for this managed instance group. Structure is documented below. For more information, see the official documentation and API
  - **distribution\_policy\_zones** - (Optional) The distribution policy for this managed instance group. You can specify one or more values. For more information, see the official documentation.
- 

The **update\_policy** block supports:

```
update_policy{
  type = "PROACTIVE"
  minimal_action = "REPLACE"
  max_surge_percent = 20
  max_unavailable_fixed = 2
  min_ready_sec = 50
}
```

- **minimal\_action** - (Required) - Minimal action to be taken on an instance. Valid values are "RESTART", "REPLACE"
- **type** - (Required) - The type of update. Valid values are "OPPORTUNISTIC", "PROACTIVE"
- **max\_surge\_fixed** - (Optional), The maximum number of instances that can be created above the specified `targetSize` during the update process. Conflicts with **max\_surge\_percent**. It has to be either 0 or at least equal to the number of zones. If fixed values are used, at least one of **max\_unavailable\_fixed** or **max\_surge\_fixed** must be greater than 0.
- **max\_surge\_percent** - (Optional), The maximum number of instances(calculated as percentage) that can be created above the specified `targetSize` during the update process. Conflicts with **max\_surge\_fixed**. Percent value is only allowed for regional managed instance groups with size at least 10.
- **max\_unavailable\_fixed** - (Optional), The maximum number of instances that can be unavailable during the update process. Conflicts with **max\_unavailable\_percent**. It has to be either 0 or at least equal to the number of zones. If fixed values are used, at least one of **max\_unavailable\_fixed** or **max\_surge\_fixed** must be greater than 0.
- **max\_unavailable\_percent** - (Optional), The maximum number of instances(calculated as percentage) that can be unavailable during the up-

date process. Conflicts with `max_unavailable_fixed`. Percent value is only allowed for regional managed instance groups with size at least 10.

- `min_ready_sec` - (Optional), Minimum number of seconds to wait for after a newly created instance becomes available. This value must be from range [0, 3600]

---

The `named_port` block supports: (Include a `named_port` block for each named-port required).

- `name` - (Required) The name of the port.
- `port` - (Required) The port number.

---

The `auto_healing_policies` block supports:

- `health_check` - (Required) The health check resource that signals auto-healing.
- `initial_delay_sec` - (Required) The number of seconds that the managed instance group waits before it applies autohealing policies to new instances or recently recreated instances. Between 0 and 3600.

The `version` block supports:

```
version {
  name = "appserver-canary"
  instance_template = "${google_compute_instance_template.appserver-canary.self_link}"
  target_size {
    fixed = 1
  }
}

version {
  name = "appserver-canary"
  instance_template = "${google_compute_instance_template.appserver-canary.self_link}"
  target_size {
    percent = 20
  }
}
```

- `name` - (Required) - Version name.
- `instance_template` - (Required) - The full URL to an instance template from which all new instances of this version will be created.
- `target_size` - (Optional) - The number of instances calculated as a fixed number or a percentage depending on the settings. Structure is documented below.

Exactly one **version** you specify must not have a **target\_size** specified. During a rolling update, the instance group manager will fulfill the **target\_size** constraints of every other **version**, and any remaining instances will be provisioned with the version where **target\_size** is unset.

The **target\_size** block supports:

- **fixed** - (Optional), The number of instances which are managed for this version. Conflicts with **percent**.
- **percent** - (Optional), The number of instances (calculated as percentage) which are managed for this version. Conflicts with **fixed**. Note that when using **percent**, rounding will be in favor of explicitly set **target\_size** values; a managed instance group with 2 instances and 2 **versions**, one of which has a **target\_size.percent** of 60 will create 2 instances of that **version**.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **fingerprint** - The fingerprint of the instance group manager.
- **instance\_group** - The full URL of the instance group created by the manager.
- **self\_link** - The URL of the created resource.

## » Import

Instance group managers can be imported using the **name**, e.g.

```
$ terraform import google_compute_region_instance_group_manager.appserver appserver-igm
```

## » google\_compute\_route

Represents a Route resource.

A route is a rule that specifies how certain packets should be handled by the virtual network. Routes are associated with virtual machines by tag, and the set of routes for a particular virtual machine is called its routing table. For each packet leaving a virtual machine, the system searches that virtual machine's routing table for a single best matching route.

Routes match packets by destination IP address, preferring smaller or more specific ranges over larger ones. If there is a tie, the system selects the route

with the smallest priority value. If there is still a tie, it uses the layer three and four packet headers to select just one of the remaining matching routes. The packet is then forwarded as specified by the `next_hop` field of the winning route -- either to another virtual machine destination, a virtual machine gateway or a Compute Engine-operated gateway. Packets that do not match any route in the sending virtual machine's routing table will be dropped.

A Route resource must have exactly one specification of either `nextHopGateway`, `nextHopInstance`, `nextHopIp`, or `nextHopVpnTunnel`.

To get more information about Route, see:

- API documentation
- How-to Guides
  - Using Routes



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Route Basic

```
resource "google_compute_route" "default" {
  name          = "network-route"
  dest_range    = "15.0.0.0/24"
  network       = "${google_compute_network.default.name}"
  next_hop_ip   = "10.132.1.5"
  priority      = 100
}

resource "google_compute_network" "default" {
  name = "compute-network"
}
```

## » Argument Reference

The following arguments are supported:

- **dest\_range** - (Required) The destination range of outgoing packets that this route applies to. Only IPv4 is supported.
- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which



means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

- **network** - (Required) The network that this route applies to.

- 
- **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.

- **priority** - (Optional) The priority of this route. Priority is used to break ties in cases where there is more than one matching route of equal prefix length. In the case of two routes with equal prefix length, the one with the lowest-numbered priority value wins. Default value is 1000. Valid range is 0 through 65535.

- **tags** - (Optional) A list of instance tags to which this route applies.

- **next\_hop\_gateway** - (Optional) URL to a gateway that should handle matching packets. Currently, you can only specify the internet gateway, using a full or partial valid URL:

- `https://www.googleapis.com/compute/v1/projects/project/global/gateways/default-internet-gateway`
  - `projects/project/global/gateways/default-internet-gateway`
  - `global/gateways/default-internet-gateway`
  - The string `default-internet-gateway`.

- **next\_hop\_instance** - (Optional) URL to an instance that should handle matching packets. You can specify this as a full or partial URL. For example:

- `https://www.googleapis.com/compute/v1/projects/project/zones/zone/instances/instance`
  - `projects/project/zones/zone/instances/instance`
  - `zones/zone/instances/instance`
  - Just the instance name, with the zone in `next_hop_instance_zone`.

- **next\_hop\_ip** - (Optional) Network IP address of an instance that should handle matching packets.

- **next\_hop\_vpn\_tunnel** - (Optional) URL to a VpnTunnel that should handle matching packets.

- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

- **next\_hop\_instance\_zone** - (Optional when **next\_hop\_instance** is specified) The zone of the instance specified in **next\_hop\_instance**. Omit if **next\_hop\_instance** is specified as a URL.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **next\_hop\_network** - URL to a Network that should handle matching packets.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

Route can be imported using any of these accepted formats:

```
$ terraform import google_compute_route.default projects/{{project}}/global/routes/{{name}}
$ terraform import google_compute_route.default {{project}}/{{name}}
$ terraform import google_compute_route.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_router

Represents a Router resource.

To get more information about Router, see:

- API documentation
- How-to Guides
  - Google Cloud Router



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Router Basic

```
resource "google_compute_router" "foobar" {
  name      = "my-router"
  network   = "${google_compute_network.foobar.name}"
  bgp {
    asn                = 64514
    advertise_mode     = "CUSTOM"
    advertised_groups   = ["ALL_SUBNETS"]
    advertised_ip_ranges {
      range = "1.2.3.4"
    }
    advertised_ip_ranges {
      range = "6.7.0.0/16"
    }
  }
}
```

```
resource "google_compute_network" "foobar" {
  name = "my-network"
  auto_create_subnetworks = false
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
  - **network** - (Required) A reference to the network to which this router belongs.
- 
- **description** - (Optional) An optional description of this resource.
  - **bgp** - (Optional) BGP information specific to this router. Structure is documented below.
  - **region** - (Optional) Region where the router resides.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **bgp** block supports:

- **asn** - (Required) Local BGP Autonomous System Number (ASN). Must be an RFC6996 private ASN, either 16-bit or 32-bit. The value will be fixed for this router resource. All VPN tunnels that link to this router will have the same local ASN.
- **advertise\_mode** - (Optional) User-specified flag to indicate which mode to use for advertisement. Valid values of this enum field are: DEFAULT, CUSTOM
- **advertised\_groups** - (Optional) User-specified list of prefix groups to advertise in custom mode. This field can only be populated if advertiseMode is CUSTOM and is advertised to all peers of the router. These groups will be advertised in addition to any specified prefixes. Leave this field blank to advertise no custom groups. This enum field has the one valid value: ALL\_SUBNETS
- **advertised\_ip\_ranges** - (Optional) User-specified list of individual IP ranges to advertise in custom mode. This field can only be populated if advertiseMode is CUSTOM and is advertised to all peers of the router. These IP ranges will be advertised in addition to any specified groups. Leave this field blank to advertise no custom IP ranges. Structure is documented below.

The **advertised\_ip\_ranges** block supports:

- **range** - (Optional) The IP range to advertise. The value must be a CIDR-formatted string.
- **description** - (Optional) User-specified description for the IP range.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

Router can be imported using any of these accepted formats:

```
$ terraform import google_compute_router.default projects/{{project}}/regions/{{region}}/routers/{{router}}
$ terraform import google_compute_router.default {{region}}/{{name}}
$ terraform import google_compute_router.default {{project}}/{{region}}/{{name}}
$ terraform import google_compute_router.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_router\_interface

Manages a Cloud Router interface. For more information see the official documentation and API.

## » Example Usage

```
resource "google_compute_router_interface" "foobar" {
  name      = "interface-1"
  router    = "router-1"
  region    = "us-central1"
  ip_range  = "169.254.1.1/30"
  vpn_tunnel = "tunnel-1"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique name for the interface, required by GCE. Changing this forces a new interface to be created.
- **router** - (Required) The name of the router this interface will be attached to. Changing this forces a new interface to be created.
- **vpn\_tunnel** - (Required) The name or resource link to the VPN tunnel this interface will be linked to. Changing this forces a new interface to be created.

- **ip\_range** - (Optional) IP address and range of the interface. The IP range must be in the RFC3927 link-local IP space. Changing this forces a new interface to be created.
- **project** - (Optional) The ID of the project in which this interface's router belongs. If it is not provided, the provider project is used. Changing this forces a new interface to be created.
- **region** - (Optional) The region this interface's router sits in. If not specified, the project region will be used. Changing this forces a new interface to be created.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » Import

Router interfaces can be imported using the **region**, **router**, and **name**, e.g.

```
$ terraform import google_compute_router_interface.foobar us-central1/router-1/interface-1
```

## » google\_compute\_router\_nat

Manages a Cloud NAT. For more information see the official documentation and API.

## » Example Usage

A simple NAT configuration: enable NAT for all Subnetworks associated with the Network associated with the given Router.

```
resource "google_compute_network" "default" {
  name = "my-network"
}

resource "google_compute_subnetwork" "default" {
  name          = "my-subnet"
  network       = "${google_compute_network.default.self_link}"
  ip_cidr_range = "10.0.0.0/16"
  region       = "us-central1"
}
```

```

resource "google_compute_router" "router" {
  name     = "router"
  region   = "${google_compute_subnetwork.default.region}"
  network  = "${google_compute_network.default.self_link}"
  bgp {
    asn = 64514
  }
}

resource "google_compute_router_nat" "simple-nat" {
  name                = "nat-1"
  router              = "${google_compute_router.router.name}"
  region              = "us-central1"
  nat_ip_allocate_option = "AUTO_ONLY"
  source_subnetwork_ip_ranges_to_nat = "ALL_SUBNETWORKS_ALL_IP_RANGES"
}

```

A production-like configuration: enable NAT for one Subnetwork and use a list of static external IP addresses.

```

resource "google_compute_network" "default" {
  name = "my-network"
}

resource "google_compute_subnetwork" "default" {
  name        = "my-subnet"
  network     = "${google_compute_network.default.self_link}"
  ip_cidr_range = "10.0.0.0/16"
  region      = "us-central1"
}

resource "google_compute_router" "router" {
  name     = "router"
  region   = "${google_compute_subnetwork.default.region}"
  network  = "${google_compute_network.default.self_link}"
  bgp {
    asn = 64514
  }
}

resource "google_compute_address" "address" {
  count = 2
  name  = "nat-external-address-${count.index}"
  region = "us-central1"
}

resource "google_compute_router_nat" "advanced-nat" {

```

```

name                    = "nat-1"
router                  = "${google_compute_router.router.name}"
region                  = "us-central1"
nat_ip_allocate_option  = "MANUAL_ONLY"
nat_ips                  = ["${google_compute_address.address.*.self_link}"]
source_subnetwork_ip_ranges_to_nat = "LIST_OF_SUBNETWORKS"
subnetwork {
  name = "${google_compute_subnetwork.subnetwork.self_link}"
}
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique name for Cloud NAT, required by GCE. Changing this forces a new NAT to be created.
  - **router** - (Required) The name of the router in which this NAT will be configured. Changing this forces a new NAT to be created.
  - **nat\_ip\_allocate\_option** - (Required) How external IPs should be allocated for this NAT. Valid values are `AUTO_ONLY` or `MANUAL_ONLY`. Changing this forces a new NAT to be created.
  - **source\_subnetwork\_ip\_ranges\_to\_nat** - (Required) How NAT should be configured per Subnetwork. Valid values include: `ALL_SUBNETWORKS_ALL_IP_RANGES`, `ALL_SUBNETWORKS_ALL_PRIMARY_IP_RANGES`, `LIST_OF_SUBNETWORKS`. Changing this forces a new NAT to be created.
- 
- **nat\_ips** - (Optional) List of `self_links` of external IPs. Only valid if `nat_ip_allocate_option` is set to `MANUAL_ONLY`. Changing this forces a new NAT to be created.
  - **subnetwork** - (Optional) One or more subnetwork NAT configurations. Only used if `source_subnetwork_ip_ranges_to_nat` is set to `LIST_OF_SUBNETWORKS`. See the section below for details on configuration.
  - **min\_ports\_per\_vm** - (Optional) Minimum number of ports allocated to a VM from this NAT config. If not set, a default number of ports is allocated to a VM. Changing this forces a new NAT to be created.
  - **udp\_idle\_timeout\_sec** - (Optional) Timeout (in seconds) for UDP connections. Defaults to 30s if not set. Changing this forces a new NAT to be created.



- `icmp_idle_timeout_sec` - (Optional) Timeout (in seconds) for ICMP connections. Defaults to 30s if not set. Changing this forces a new NAT to be created.
- `tcp_established_idle_timeout_sec` - (Optional) Timeout (in seconds) for TCP established connections. Defaults to 1200s if not set. Changing this forces a new NAT to be created.
- `tcp_transitory_idle_timeout_sec` - (Optional) Timeout (in seconds) for TCP transitory connections. Defaults to 30s if not set. Changing this forces a new NAT to be created.
- `project` - (Optional) The ID of the project in which this NAT's router belongs. If it is not provided, the provider project is used. Changing this forces a new NAT to be created.
- `region` - (Optional) The region this NAT's router sits in. If not specified, the project region will be used. Changing this forces a new NAT to be created.

The `subnetwork` block supports:

- `name` - (Required) The `self_link` of the subnetwork to NAT.
- `source_ip_ranges_to_nat` - (Required) List of options for which source IPs in the subnetwork should have NAT enabled. Supported values include: `ALL_IP_RANGES`, `LIST_OF_SECONDARY_IP_RANGES`, `PRIMARY_IP_RANGE`
- `secondary_ip_range_names` - (Optional) List of the secondary ranges of the subnetwork that are allowed to use NAT. This can be populated only if `LIST_OF_SECONDARY_IP_RANGES` is one of the values in `source_ip_ranges_to_nat`.

## » Import

Router NATs can be imported using the `region`, `router`, and `name`, e.g.

```
$ terraform import google_compute_router_nat.my-nat us-central1/router-1/nat-1
```

## » `google_compute_router_peer`

Manages a Cloud Router BGP peer. For more information see the official documentation and API.

## » Example Usage

```
resource "google_compute_router_peer" "foobar" {
  name                = "peer-1"
  router              = "router-1"
  region              = "us-central1"
  peer_ip_address     = "169.254.1.2"
  peer_asn            = 65513
  advertised_route_priority = 100
  interface           = "interface-1"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique name for BGP peer, required by GCE. Changing this forces a new peer to be created.
  - **router** - (Required) The name of the router in which this BGP peer will be configured. Changing this forces a new peer to be created.
  - **interface** - (Required) The name of the interface the BGP peer is associated with. Changing this forces a new peer to be created.
  - **peer\_ip\_address** - (Required) IP address of the BGP interface outside Google Cloud. Changing this forces a new peer to be created.
  - **peer\_asn** - (Required) Peer BGP Autonomous System Number (ASN). Changing this forces a new peer to be created.
- 
- **advertised\_route\_priority** - (Optional) The priority of routes advertised to this BGP peer. Changing this forces a new peer to be created.
  - **project** - (Optional) The ID of the project in which this peer's router belongs. If it is not provided, the provider project is used. Changing this forces a new peer to be created.
  - **region** - (Optional) The region this peer's router sits in. If not specified, the project region will be used. Changing this forces a new peer to be created.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `ip_address` - IP address of the interface inside Google Cloud Platform.

## » Import

Router BGP peers can be imported using the `region`, `router`, and `name`, e.g.

```
$ terraform import google_compute_router_peer.foobar us-central1/router-1/peer-1
```

## » `google_compute_security_policy`

A Security Policy defines an IP blacklist or whitelist that protects load balanced Google Cloud services by denying or permitting traffic from specified IP ranges. For more information see the official documentation and the API.

## » Example Usage

```
resource "google_compute_security_policy" "policy" {
  name = "my-policy"

  rule {
    action    = "deny(403)"
    priority  = "1000"
    match {
      versioned_expr = "SRC_IPS_V1"
      config {
        src_ip_ranges = ["9.9.9.0/24"]
      }
    }
    description = "Deny access to IPs in 9.9.9.0/24"
  }

  rule {
    action    = "allow"
    priority  = "2147483647"
    match {
      versioned_expr = "SRC_IPS_V1"
      config {
        src_ip_ranges = ["*"]
      }
    }
    description = "default rule"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the security policy.
- 
- **description** - (Optional) An optional description of this security policy. Max size is 2048.
  - **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
  - **rule** - (Optional) The set of rules that belong to this policy. There must always be a default rule (rule with priority 2147483647 and match `""`). If no rules are provided when creating a security policy, a default rule with action `"allow"` will be added. Structure is documented below.

The **rule** block supports:

- **action** - (Required) Action to take when **match** matches the request. Valid values:
  - `"allow"` : allow access to target
  - `"deny(status)"` : deny access to target, returns the HTTP response code specified (valid values are 403, 404 and 502)
- **priority** - (Required) An unique positive integer indicating the priority of evaluation for a rule. Rules are evaluated from highest priority (lowest numerically) to lowest priority (highest numerically) in order.
- **match** - (Required) A match condition that incoming traffic is evaluated against. If it evaluates to true, the corresponding **action** is enforced. Structure is documented below.
- **description** - (Optional) An optional description of this rule. Max size is 64.
- **preview** - (Optional) When set to true, the **action** specified above is not enforced. Stackdriver logs for requests that trigger a preview action are annotated as such.

The **match** block supports:

- **config** - (Required) The configuration options available when specifying **versioned\_expr**. Structure is documented below.
- **versioned\_expr** - (Required) Predefined rule expression. Available options:
  - **SRC\_IPS\_V1**: Must specify the corresponding **src\_ip\_ranges** field in **config**.

The `config` block supports:

- `src_ip_ranges` - (Required) Set of IP addresses or ranges (IPv4 or IPv6) in CIDR notation to match against inbound traffic. There is a limit of 5 IP ranges per rule. A value of '\*' matches all IPs (can be used to override the default behavior).

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `fingerprint` - Fingerprint of this resource.
- `self_link` - The URI of the created resource.

## » Import

Security policies can be imported using the `name`, e.g.

```
$ terraform import google_compute_security_policy.policy my-policy
```

## » google\_compute\_shared\_vpc\_host\_project

Enables the Google Compute Engine Shared VPC feature for a project, assigning it as a Shared VPC host project.

For more information, see, the Project API documentation, where the Shared VPC feature is referred to by its former name "XPN".

## » Example Usage

```
# A host project provides network resources to associated service projects.
resource "google_compute_shared_vpc_host_project" "host" {
  project = "host-project-id"
}

# A service project gains access to network resources provided by its
# associated host project.
resource "google_compute_shared_vpc_service_project" "service1" {
  host_project      = "${google_compute_shared_vpc_host_project.host.project}"
  service_project = "service-project-id-1"
}
resource "google_compute_shared_vpc_service_project" "service2" {
```

```

    host_project      = "${google_compute_shared_vpc_host_project.host.project}"
    service_project = "service-project-id-2"
}

```

## » Argument Reference

The following arguments are expected:

- **project** - (Required) The ID of the project that will serve as a Shared VPC host project

## » Import

Google Compute Engine Shared VPC host project feature can be imported using the **project**, e.g.

```
$ terraform import google_compute_shared_vpc_host_project.host host-project-id
```

## » google\_compute\_shared\_vpc\_service\_project

Enables the Google Compute Engine Shared VPC feature for a project, assigning it as a Shared VPC service project associated with a given host project.

For more information, see, the Project API documentation, where the Shared VPC feature is referred to by its former name "XPN".

## » Example Usage

```

resource "google_compute_shared_vpc_service_project" "service1" {
    host_project      = "host-project-id"
    service_project = "service-project-id-1"
}

```

For a complete Shared VPC example with both host and service projects, see `google_compute_shared_vpc_host_project`.

## » Argument Reference

The following arguments are expected:

- **host\_project** - (Required) The ID of a host project to associate.
- **service\_project** - (Required) The ID of the project that will serve as a Shared VPC service project.

## » Import

Google Compute Engine Shared VPC service project feature can be imported using the `host_project` and `service_project`, e.g.

```
$ terraform import google_compute_shared_vpc_service_project.service1 host-project-id/service-project-id
```

## » google\_compute\_snapshot

Represents a Persistent Disk Snapshot resource.

Use snapshots to back up data from your persistent disks. Snapshots are different from public images and custom images, which are used primarily to create instances or configure instance templates. Snapshots are useful for periodic backup of the data on your persistent disks. You can create snapshots from persistent disks even while they are attached to running instances.

Snapshots are incremental, so you can create regular snapshots on a persistent disk faster and at a much lower cost than if you regularly created a full image of the disk.

To get more information about Snapshot, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Snapshot Basic

```
resource "google_compute_snapshot" "snapshot" {
  name = "my-snapshot"
  source_disk = "${google_compute_disk.persistent.name}"
  zone = "us-central1-a"
  labels = {
    my_label = "value"
  }
}

data "google_compute_image" "debian" {
  family = "debian-9"
```

```

    project = "debian-cloud"
  }

  resource "google_compute_disk" "persistent" {
    name = "debian-disk"
    image = "${data.google_compute_image.debian.self_link}"
    size = 10
    type = "pd-ssd"
    zone = "us-central1-a"
  }

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource; provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
  - **source\_disk** - (Required) A reference to the disk used to create this snapshot.
- 
- **description** - (Optional) An optional description of this resource.
  - **labels** - (Optional) Labels to apply to this Snapshot.
  - **zone** - (Optional) A reference to the zone where the disk is hosted.
  - **snapshot\_encryption\_key** - (Optional) The customer-supplied encryption key of the snapshot. Required if the source snapshot is protected by a customer-supplied encryption key. Structure is documented below.
  - **source\_disk\_encryption\_key** - (Optional) The customer-supplied encryption key of the source snapshot. Required if the source snapshot is protected by a customer-supplied encryption key. Structure is documented below.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The `snapshot_encryption_key` block supports:

- **raw\_key** - (Optional) Specifies a 256-bit customer-supplied encryption key, encoded in RFC 4648 base64 to either encrypt or decrypt this resource.



- **sha256** - The RFC 4648 base64 encoded SHA-256 hash of the customer-supplied encryption key that protects this resource.

The **source\_disk\_encryption\_key** block supports:

- **raw\_key** - (Optional) Specifies a 256-bit customer-supplied encryption key, encoded in RFC 4648 base64 to either encrypt or decrypt this resource.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **snapshot\_id** - The unique identifier for the resource.
- **disk\_size\_gb** - Size of the snapshot, specified in GB.
- **storage\_bytes** - A size of the the storage used by the snapshot. As snapshots share storage, this number is expected to change with snapshot creation/deletion.
- **licenses** - A list of public visible licenses that apply to this snapshot. This can be because the original image had licenses attached (such as a Windows image). `snapshotEncryptionKey` nested object Encrypts the snapshot using a customer-supplied encryption key.
- **label\_fingerprint** - The fingerprint used for optimistic locking of this resource. Used internally during updates.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 5 minutes.
- **update** - Default is 5 minutes.
- **delete** - Default is 5 minutes.

## » Import

Snapshot can be imported using any of these accepted formats:

```
$ terraform import google_compute_snapshot.default projects/{{project}}/global/snapshots/{{name}}
$ terraform import google_compute_snapshot.default {{project}}/{{name}}
$ terraform import google_compute_snapshot.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_compute_managed_ssl_certificate`

An `SslCertificate` resource, used for HTTPS load balancing. This resource represents a certificate for which the certificate secrets are created and managed by Google.

For a resource where you provide the key, see the `SSL Certificate` resource.

**Warning:** This resource is in beta, and should be used with the `terraform-provider-google-beta` provider. See [Provider Versions](#) for more details on beta resources.

To get more information about `ManagedSslCertificate`, see:

- [API documentation](#)
- [How-to Guides](#)
  - [Official Documentation](#)

**Warning:** This resource should be used with extreme caution! Provisioning an SSL certificate is complex. Ensure that you understand the lifecycle of a certificate before attempting complex tasks like cert rotation automatically. This resource will "return" as soon as the certificate object is created, but post-creation the certificate object will go through a "provisioning" process. The provisioning process can complete only when the domain name for which the certificate is created points to a target pool which, itself, points at the certificate. Depending on your DNS provider, this may take some time, and migrating from self-managed certificates to Google-managed certificates may entail some downtime while the certificate provisions.

In conclusion: Be extremely cautious.



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Managed Ssl Certificate Basic

```
resource "google_compute_managed_ssl_certificate" "default" {  
  provider = "google-beta"  
  
  name = "test-cert"
```

```

    managed {
      domains = ["sslcert.tf-test.club"]
    }
  }

resource "google_compute_target_https_proxy" "default" {
  provider = "google-beta"

  name          = "test-proxy"
  url_map       = "${google_compute_url_map.default.self_link}"
  ssl_certificates = ["${google_compute_managed_ssl_certificate.default.self_link}"]
}

resource "google_compute_url_map" "default" {
  provider = "google-beta"

  name          = "url-map"
  description   = "a description"

  default_service = "${google_compute_backend_service.default.self_link}"

  host_rule {
    hosts      = ["sslcert.tf-test.club"]
    path_matcher = "allpaths"
  }

  path_matcher {
    name          = "allpaths"
    default_service = "${google_compute_backend_service.default.self_link}"

    path_rule {
      paths      = ["/*"]
      service    = "${google_compute_backend_service.default.self_link}"
    }
  }
}

resource "google_compute_backend_service" "default" {
  provider = "google-beta"

  name          = "backend-service"
  port_name     = "http"
  protocol      = "HTTP"
  timeout_sec   = 10

```

```

    health_checks = ["${google_compute_http_health_check.default.self_link}"]
}

resource "google_compute_http_health_check" "default" {
    provider = "google-beta"

    name           = "http-health-check"
    request_path    = "/"
    check_interval_sec = 1
    timeout_sec     = 1
}

resource "google_dns_managed_zone" "zone" {
    provider = "google-beta"

    name      = "dnszone"
    dns_name = "sslcert.tf-test.club."
}

resource "google_compute_global_forwarding_rule" "default" {
    provider = "google-beta"

    name      = "forwarding-rule"
    target     = "${google_compute_target_https_proxy.default.self_link}"
    port_range = 443
}

resource "google_dns_record_set" "set" {
    provider = "google-beta"

    name      = "sslcert.tf-test.club."
    type      = "A"
    ttl       = 3600
    managed_zone = "${google_dns_managed_zone.zone.name}"
    rrdatas    = ["${google_compute_global_forwarding_rule.default.ip_address}"]
}

provider "google-beta" {
    region = "us-central1"
    zone   = "us-central1-a"
}

```

## » Argument Reference

The following arguments are supported:

- 
- **description** - (Optional) An optional description of this resource.
  - **name** - (Optional) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

These are in the same namespace as the managed SSL certificates.

- **managed** - (Optional) Properties relevant to a managed certificate. These will be used if the certificate is managed (as indicated by a value of **MANAGED** in **type**). Structure is documented below.
- **type** - (Optional) Specifies the type of SSL certificate, either **SELF\_MANAGED** or **MANAGED**. If not specified, the certificate is self-managed.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **managed** block supports:

- **domains** - (Required) Domains for which a managed SSL certificate will be valid. Currently, there can only be one domain in this list.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **certificate\_id** - The unique identifier for the resource.
- **subject\_alternative\_names** - Domains associated with the certificate via Subject Alternative Name.
- **expire\_time** - Expire time of the certificate.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 6 minutes.
- **delete** - Default is 30 minutes.

## » Import

ManagedSslCertificate can be imported using any of these accepted formats:

```
$ terraform import -provider=google-beta google_compute_managed_ssl_certificate.default proj
$ terraform import -provider=google-beta google_compute_managed_ssl_certificate.default {{pr
$ terraform import -provider=google-beta google_compute_managed_ssl_certificate.default {{na
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_compute\_\_ssl\_\_certificate

An SslCertificate resource, used for HTTPS load balancing. This resource provides a mechanism to upload an SSL key and certificate to the load balancer to serve secure connections from the user.

To get more information about SslCertificate, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Ssl Certificate Basic

```
resource "google_compute_ssl_certificate" "default" {
  name_prefix = "my-certificate-"
  description = "a description"
  private_key = "${file("path/to/private.key")}"
  certificate = "${file("path/to/certificate.crt")}"

  lifecycle {
    create_before_destroy = true
  }
}
```



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Ssl Certificate Random Provider

```
# You may also want to control name generation explicitly:
resource "google_compute_ssl_certificate" "default" {
  # The name will contain 8 random hex digits,
  # e.g. "my-certificate-48ab27cd2a"
  name          = "${random_id.certificate.hex}"
  private_key   = "${file("path/to/private.key")}"
  certificate    = "${file("path/to/certificate.crt")}"

  lifecycle {
    create_before_destroy = true
  }
}

resource "random_id" "certificate" {
  byte_length = 4
  prefix      = "my-certificate-"

  # For security, do not expose raw certificate values in the output
  keepers = {
    private_key = "${base64sha256(file("path/to/private.key"))}"
    certificate  = "${base64sha256(file("path/to/certificate.crt"))}"
  }
}
```



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Ssl Certificate Target Https Proxies

```
// Using with Target HTTPS Proxies
//
// SSL certificates cannot be updated after creation. In order to apply
// the specified configuration, Terraform will destroy the existing
// resource and create a replacement. To effectively use an SSL
```

```

// certificate resource with a Target HTTPS Proxy resource, it's
// recommended to specify create_before_destroy in a lifecycle block.
// Either omit the Instance Template name attribute, specify a partial
// name with name_prefix, or use random_id resource. Example:

resource "google_compute_ssl_certificate" "default" {
  name_prefix = "my-certificate-"
  private_key = "${file("path/to/private.key")}"
  certificate = "${file("path/to/certificate.crt")}"

  lifecycle {
    create_before_destroy = true
  }
}

resource "google_compute_target_https_proxy" "default" {
  name          = "test-proxy"
  url_map       = "${google_compute_url_map.default.self_link}"
  ssl_certificates = ["${google_compute_ssl_certificate.default.self_link}"]
}

resource "google_compute_url_map" "default" {
  name          = "url-map"
  description   = "a description"

  default_service = "${google_compute_backend_service.default.self_link}"

  host_rule {
    hosts      = ["mysite.com"]
    path_matcher = "allpaths"
  }

  path_matcher {
    name          = "allpaths"
    default_service = "${google_compute_backend_service.default.self_link}"

    path_rule {
      paths      = ["/*"]
      service    = "${google_compute_backend_service.default.self_link}"
    }
  }
}

resource "google_compute_backend_service" "default" {
  name          = "backend-service"
  port_name     = "http"

```



```

protocol      = "HTTP"
timeout_sec   = 10

health_checks = ["${google_compute_http_health_check.default.self_link}"]
}

resource "google_compute_http_health_check" "default" {
  name           = "http-health-check"
  request_path    = "/"
  check_interval_sec = 1
  timeout_sec     = 1
}

```

## » Argument Reference

The following arguments are supported:

- **certificate** - (Required) The certificate in PEM format. The certificate chain must be no greater than 5 certs long. The chain must include at least one intermediate cert.
  - **private\_key** - (Required) The write-only private key in PEM format.
- 
- **description** - (Optional) An optional description of this resource.
  - **name** - (Optional) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

These are in the same namespace as the managed SSL certificates. \* **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

- **name\_prefix** - (Optional) Creates a unique name beginning with the specified prefix. Conflicts with **name**.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.

- `certificate_id` - The unique identifier for the resource.
- `self_link` - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

SslCertificate can be imported using any of these accepted formats:

```
$ terraform import google_compute_ssl_certificate.default projects/{{project}}/global/sslCertificate/{{name}}
$ terraform import google_compute_ssl_certificate.default {{project}}/{{name}}
$ terraform import google_compute_ssl_certificate.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_ssl\_policy

Represents a SSL policy. SSL policies give you the ability to control the features of SSL that your SSL proxy or HTTPS load balancer negotiates.

To get more information about SslPolicy, see:

- API documentation
- How-to Guides
  - Using SSL Policies



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Ssl Policy Basic

```
resource "google_compute_ssl_policy" "prod-ssl-policy" {
  name      = "production-ssl-policy"
  profile   = "MODERN"
```

```

}

resource "google_compute_ssl_policy" "nonprod-ssl-policy" {
  name          = "nonprod-ssl-policy"
  profile       = "MODERN"
  min_tls_version = "TLS_1_2"
}

resource "google_compute_ssl_policy" "custom-ssl-policy" {
  name          = "custom-ssl-policy"
  min_tls_version = "TLS_1_2"
  profile       = "CUSTOM"
  custom_features = ["TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_AES_256_
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- 
- **description** - (Optional) An optional description of this resource.
  - **profile** - (Optional) Profile specifies the set of SSL features that can be used by the load balancer when negotiating SSL with clients. This can be one of `COMPATIBLE`, `MODERN`, `RESTRICTED`, or `CUSTOM`. If using `CUSTOM`, the set of SSL features to enable must be specified in the `customFeatures` field. See the official documentation for information on what cipher suites each profile provides. If `CUSTOM` is used, the `custom_features` attribute **must be set**. Default is `COMPATIBLE`.
  - **min\_tls\_version** - (Optional) The minimum version of SSL protocol that can be used by the clients to establish a connection with the load balancer. This can be one of `TLS_1_0`, `TLS_1_1`, `TLS_1_2`. Default is `TLS_1_0`.
  - **custom\_features** - (Optional) Profile specifies the set of SSL features that can be used by the load balancer when negotiating SSL with clients. This can be one of `COMPATIBLE`, `MODERN`, `RESTRICTED`, or `CUSTOM`. If using `CUSTOM`, the set of SSL features to enable must be specified in the `customFeatures` field. See the official documentation for which ciphers

are available to use. **Note:** this argument *must* be present when using the **CUSTOM** profile. This argument *must not* be present when using any other profile.

- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **enabled\_features** - The list of features enabled in the SSL policy.
- **fingerprint** - Fingerprint of this resource. A hash of the contents stored in this object. This field is used in optimistic locking.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

SslPolicy can be imported using any of these accepted formats:

```
$ terraform import google_compute_ssl_policy.default projects/{{project}}/global/sslPolicies/{{name}}
$ terraform import google_compute_ssl_policy.default {{project}}/{{name}}
$ terraform import google_compute_ssl_policy.default {{name}}
```

If you're importing a resource with beta features, make sure to include **-provider=google-beta** as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_subnetwork

A VPC network is a virtual version of the traditional physical networks that exist within and between physical data centers. A VPC network provides connectivity

for your Compute Engine virtual machine (VM) instances, Container Engine containers, App Engine Flex services, and other network-related resources.

Each GCP project contains one or more VPC networks. Each VPC network is a global entity spanning all GCP regions. This global VPC network allows VM instances and other resources to communicate with each other via internal, private IP addresses.

Each VPC network is subdivided into subnets, and each subnet is contained within a single region. You can have more than one subnet in a region for a given VPC network. Each subnet has a contiguous private RFC1918 IP space. You create instances, containers, and the like in these subnets. When you create an instance, you must create it in a subnet, and the instance draws its internal IP address from that subnet.

Virtual machine (VM) instances in a VPC network can communicate with instances in all other subnets of the same VPC network, regardless of region, using their RFC1918 private IP addresses. You can isolate portions of the network, even entire subnets, using firewall rules.

To get more information about Subnetwork, see:

- API documentation
- How-to Guides
  - Private Google Access
  - Cloud Networking



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Subnetwork Basic

```
resource "google_compute_subnetwork" "network-with-private-secondary-ip-ranges" {
  name           = "test-subnetwork"
  ip_cidr_range  = "10.2.0.0/16"
  region         = "us-central1"
  network        = "${google_compute_network.custom-test.self_link}"
  secondary_ip_range {
    range_name    = "tf-test-secondary-range-update1"
    ip_cidr_range = "192.168.10.0/24"
  }
}

resource "google_compute_network" "custom-test" {
  name = "test-network"
```

```

    auto_create_subnetworks = false
}

```

## » Argument Reference

The following arguments are supported:

- **ip\_cidr\_range** - (Required) The range of internal addresses that are owned by this subnetwork. Provide this property when you create the subnetwork. For example, 10.0.0.0/8 or 192.168.0.0/16. Ranges must be unique and non-overlapping within a network. Only IPv4 is supported.
- **name** - (Required) The name of the resource, provided by the client when initially creating the resource. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- **network** - (Required) The network this subnet belongs to. Only networks that are in the distributed mode can have subnetworks.

- 
- **description** - (Optional) An optional description of this resource. Provide this property when you create the resource. This field can be set only at resource creation time.
  - **enable\_flow\_logs** - (Optional) Whether to enable flow logging for this subnetwork.
  - **secondary\_ip\_range** - (Optional) An array of configurations for secondary IP ranges for VM instances contained in this subnetwork. The primary IP of such VM must belong to the primary `ipCidrRange` of the subnetwork. The alias IPs may belong to either primary or secondary ranges. Structure is documented below.
  - **private\_ip\_google\_access** - (Optional) When enabled, VMs in this subnetwork without external IP addresses can access Google APIs and services by using Private Google Access.
  - **region** - (Optional) URL of the GCP region for this subnetwork.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **secondary\_ip\_range** block supports:

- **range\_name** - (Required) The name associated with this subnetwork secondary range, used when adding an alias IP range to a VM instance. The

name must be 1-63 characters long, and comply with RFC1035. The name must be unique within the subnetwork.

- **ip\_cidr\_range** - (Required) The range of IP addresses belonging to this subnetwork secondary range. Provide this property when you create the subnetwork. Ranges must be unique and non-overlapping with all primary and secondary IP ranges within a network. Only IPv4 is supported.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **gateway\_address** - The gateway address for default routes to reach destination addresses outside this subnetwork.
- **fingerprint** - Fingerprint of this resource. This field is used internally during updates of this resource.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 6 minutes.
- **update** - Default is 6 minutes.
- **delete** - Default is 6 minutes.

## » Import

Subnetwork can be imported using any of these accepted formats:

```
$ terraform import google_compute_subnetwork.default projects/{{project}}/regions/{{region}}
$ terraform import google_compute_subnetwork.default {{region}}/{{name}}
$ terraform import google_compute_subnetwork.default {{project}}/{{region}}/{{name}}
$ terraform import google_compute_subnetwork.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » IAM policy for GCE subnetwork

**Warning:** These resources are in beta, and should be used with the terraform-provider-google-beta provider. See Provider Versions for more details on beta resources.

Three different resources help you manage your IAM policy for GCE subnetwork. Each of these resources serves a different use case:

- `google_compute_subnetwork_iam_policy`: Authoritative. Sets the IAM policy for the subnetwork and replaces any existing policy already attached.
- `google_compute_subnetwork_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the subnetwork are preserved.
- `google_compute_subnetwork_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the subnetwork are preserved.

**Note:** `google_compute_subnetwork_iam_policy` **cannot** be used in conjunction with `google_compute_subnetwork_iam_binding` and `google_compute_subnetwork_iam_member` or they will fight over what your policy should be.

**Note:** `google_compute_subnetwork_iam_binding` resources **can be** used in conjunction with `google_compute_subnetwork_iam_member` resources **only if** they do not grant privilege to the same role.

## » `google_compute_subnetwork_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_compute_subnetwork_iam_policy" "subnet" {
  subnetwork = "your-subnetwork-id"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```



## » google\_compute\_subnetwork\_iam\_binding

```
resource "google_compute_subnetwork_iam_binding" "subnet" {
  subnetwork = "your-subnetwork-id"
  role       = "roles/compute.networkUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_compute\_subnetwork\_iam\_member

```
resource "google_compute_subnetwork_iam_member" "subnet" {
  subnetwork = "your-subnetwork-id"
  role       = "roles/compute.networkUser"
  member     = "user:jane@example.com"
}
```

## » Argument Reference

The following arguments are supported:

- **subnetwork** - (Required) The name of the subnetwork.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_compute_subnetwork_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.

- **policy\_data** - (Required only by `google_compute_subnetwork_iam_policy`)  
The policy data generated by a `google_iam_policy` data source.
- **project** - (Optional) The ID of the project in which the resource belongs.  
If it is not provided, the provider project is used.
- **region** - (Optional) The region of the subnetwork. If unspecified, this defaults to the region configured in the provider.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the subnetwork's IAM policy.

## » Import

For all import syntaxes, the "resource in question" can take any of the following forms:

- full self link or relative link (`projects/{{project}}/region/{{region}}/subnetworks/{{name}}`)
- `{{project}}/{{region}}/{{name}}`
- `{{region}}/{{name}}` (project is taken from provider project)
- `{{name}}` (project and region are taken from provider project)

IAM member imports use space-delimited identifiers; the resource in question, the role, and the member identity, e.g.

```
$ terraform import google_compute_subnetwork_iam_member.subnet "project-name/region-name/subnet-name/role-name/member-name"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role, e.g.

```
$ terraform import google_compute_subnetwork_iam_binding.subnet "project-name/region-name/subnet-name/role-name"
```

IAM policy imports use the identifier of the resource in question, e.g.

```
$ terraform import google_compute_subnetwork_iam_policy.subnet project-name/region-name/subnet-name
```

## » IAM policy for GCE subnetwork

**Warning:** These resources are in beta, and should be used with the `terraform-provider-google-beta` provider. See [Provider Versions](#) for more details on beta resources.

Three different resources help you manage your IAM policy for GCE subnetwork. Each of these resources serves a different use case:

- `google_compute_subnetwork_iam_policy`: Authoritative. Sets the IAM policy for the subnetwork and replaces any existing policy already attached.
- `google_compute_subnetwork_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the subnetwork are preserved.
- `google_compute_subnetwork_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the subnetwork are preserved.

**Note:** `google_compute_subnetwork_iam_policy` **cannot** be used in conjunction with `google_compute_subnetwork_iam_binding` and `google_compute_subnetwork_iam_member` or they will fight over what your policy should be.

**Note:** `google_compute_subnetwork_iam_binding` resources **can be** used in conjunction with `google_compute_subnetwork_iam_member` resources **only if** they do not grant privilege to the same role.

## » `google_compute_subnetwork_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_compute_subnetwork_iam_policy" "subnet" {
  subnetwork = "your-subnetwork-id"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

## » `google_compute_subnetwork_iam_binding`

```
resource "google_compute_subnetwork_iam_binding" "subnet" {
  subnetwork = "your-subnetwork-id"
  role       = "roles/compute.networkUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\compute\_subnetwork\_iam\_member

```
resource "google_compute_subnetwork_iam_member" "subnet" {  
  subnetwork = "your-subnetwork-id"  
  role       = "roles/compute.networkUser"  
  member     = "user:jane@example.com"  
}
```

## » Argument Reference

The following arguments are supported:

- **subnetwork** - (Required) The name of the subnetwork.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_compute_subnetwork_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_compute_subnetwork_iam_policy`) The policy data generated by a `google_iam_policy` data source.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **region** - (Optional) The region of the subnetwork. If unspecified, this defaults to the region configured in the provider.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the subnetwork's IAM policy.

## » Import

For all import syntaxes, the "resource in question" can take any of the following forms:

- full self link or relative link (projects/{{project}}/region/{{region}}/subnetworks/{{name}})
- {{project}}/{{region}}/{{name}}
- {{region}}/{{name}} (project is taken from provider project)
- {{name}} (project and region are taken from provider project)

IAM member imports use space-delimited identifiers; the resource in question, the role, and the member identity, e.g.

```
$ terraform import google_compute_subnetwork_iam_member.subnet "project-name/region-name/subnet-name/role-name/member-name"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role, e.g.

```
$ terraform import google_compute_subnetwork_iam_binding.subnet "project-name/region-name/subnet-name/role-name"
```

IAM policy imports use the identifier of the resource in question, e.g.

```
$ terraform import google_compute_subnetwork_iam_policy.subnet project-name/region-name/subnet-name
```

## » IAM policy for GCE subnetwork

**Warning:** These resources are in beta, and should be used with the terraform-provider-google-beta provider. See Provider Versions for more details on beta resources.

Three different resources help you manage your IAM policy for GCE subnetwork. Each of these resources serves a different use case:

- **google\_compute\_subnetwork\_iam\_policy:** Authoritative. Sets the IAM policy for the subnetwork and replaces any existing policy already attached.
- **google\_compute\_subnetwork\_iam\_binding:** Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the subnetwork are preserved.

- `google_compute_subnetwork_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the subnetwork are preserved.

**Note:** `google_compute_subnetwork_iam_policy` **cannot** be used in conjunction with `google_compute_subnetwork_iam_binding` and `google_compute_subnetwork_iam_member` or they will fight over what your policy should be.

**Note:** `google_compute_subnetwork_iam_binding` resources **can be** used in conjunction with `google_compute_subnetwork_iam_member` resources **only if** they do not grant privilege to the same role.

## » `google_compute_subnetwork_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_compute_subnetwork_iam_policy" "subnet" {
  subnetwork = "your-subnetwork-id"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

## » `google_compute_subnetwork_iam_binding`

```
resource "google_compute_subnetwork_iam_binding" "subnet" {
  subnetwork = "your-subnetwork-id"
  role       = "roles/compute.networkUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » `google_compute_subnetwork_iam_member`

```
resource "google_compute_subnetwork_iam_member" "subnet" {
  subnetwork = "your-subnetwork-id"
```

```

    role      = "roles/compute.networkUser"
    member    = "user:jane@example.com"
  }

```

## » Argument Reference

The following arguments are supported:

- **subnetwork** - (Required) The name of the subnetwork.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, alice@gmail.com or joe@example.com.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_compute_subnetwork_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_compute_subnetwork_iam_policy`) The policy data generated by a `google_iam_policy` data source.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **region** - (Optional) The region of the subnetwork. If unspecified, this defaults to the region configured in the provider.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the subnetwork's IAM policy.

## » Import

For all import syntaxes, the "resource in question" can take any of the following forms:

- full self link or relative link (projects/{{project}}/region/{{region}}/subnetworks/{{name}})
- {{project}}/{{region}}/{{name}}
- {{region}}/{{name}} (project is taken from provider project)
- {{name}} (project and region are taken from provider project)

IAM member imports use space-delimited identifiers; the resource in question, the role, and the member identity, e.g.

```
$ terraform import google_compute_subnetwork_iam_member.subnet "project-name/region-name/subnet-name/role/identity"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role, e.g.

```
$ terraform import google_compute_subnetwork_iam_binding.subnet "project-name/region-name/subnet-name/role/identity"
```

IAM policy imports use the identifier of the resource in question, e.g.

```
$ terraform import google_compute_subnetwork_iam_policy.subnet project-name/region-name/subnet-name
```

## » google\_compute\_target\_http\_proxy

Represents a TargetHttpProxy resource, which is used by one or more global forwarding rule to route incoming HTTP requests to a URL map.

To get more information about TargetHttpProxy, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Target Http Proxy Basic

```
resource "google_compute_target_http_proxy" "default" {
  name        = "test-proxy"
  url_map     = "${google_compute_url_map.default.self_link}"
}
```



```

resource "google_compute_url_map" "default" {
  name          = "url-map"
  default_service = "${google_compute_backend_service.default.self_link}"

  host_rule {
    hosts      = ["mysite.com"]
    path_matcher = "allpaths"
  }

  path_matcher {
    name          = "allpaths"
    default_service = "${google_compute_backend_service.default.self_link}"

    path_rule {
      paths      = ["/*"]
      service = "${google_compute_backend_service.default.self_link}"
    }
  }
}

resource "google_compute_backend_service" "default" {
  name          = "backend-service"
  port_name     = "http"
  protocol      = "HTTP"
  timeout_sec   = 10

  health_checks = ["${google_compute_http_health_check.default.self_link}"]
}

resource "google_compute_http_health_check" "default" {
  name          = "http-health-check"
  request_path   = "/"
  check_interval_sec = 1
  timeout_sec    = 1
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following char-

acters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

- **url\_map** - (Required) A reference to the UrlMap resource that defines the mapping from URL to the BackendService.

- 
- **description** - (Optional) An optional description of this resource.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **proxy\_id** - The unique identifier for the resource.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

TargetHttpProxy can be imported using any of these accepted formats:

```
$ terraform import google_compute_target_http_proxy.default projects/{{project}}/global/targetHttpProxies/{{name}}
$ terraform import google_compute_target_http_proxy.default {{project}}/{{name}}
$ terraform import google_compute_target_http_proxy.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_target\_https\_proxy

Represents a TargetHttpsProxy resource, which is used by one or more global forwarding rule to route incoming HTTPS requests to a URL map.

To get more information about TargetHttpsProxy, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

### » Example Usage - Target Https Proxy Basic

```
resource "google_compute_target_https_proxy" "default" {
  name          = "test-proxy"
  url_map       = "${google_compute_url_map.default.self_link}"
  ssl_certificates = ["${google_compute_ssl_certificate.default.self_link}"]
}

resource "google_compute_ssl_certificate" "default" {
  name          = "my-certificate"
  private_key   = "${file("path/to/private.key")}"
  certificate   = "${file("path/to/certificate.crt")}"
}

resource "google_compute_url_map" "default" {
  name          = "url-map"
  description   = "a description"

  default_service = "${google_compute_backend_service.default.self_link}"

  host_rule {
    hosts          = ["mysite.com"]
    path_matcher   = "allpaths"
  }

  path_matcher {
    name          = "allpaths"
    default_service = "${google_compute_backend_service.default.self_link}"
  }
}
```

```

    path_rule {
      paths    = ["/*"]
      service = "${google_compute_backend_service.default.self_link}"
    }
  }
}

resource "google_compute_backend_service" "default" {
  name          = "backend-service"
  port_name     = "http"
  protocol      = "HTTP"
  timeout_sec   = 10

  health_checks = ["${google_compute_http_health_check.default.self_link}"]
}

resource "google_compute_http_health_check" "default" {
  name          = "http-health-check"
  request_path   = "/"
  check_interval_sec = 1
  timeout_sec    = 1
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
  - **ssl\_certificates** - (Required) A list of SslCertificate resources that are used to authenticate connections between users and the load balancer. Currently, exactly one SSL certificate must be specified.
  - **url\_map** - (Required) A reference to the UrlMap resource that defines the mapping from URL to the BackendService.
- 
- **description** - (Optional) An optional description of this resource.
  - **quic\_override** - (Optional) Specifies the QUIC override policy for this resource. This determines whether the load balancer will attempt to ne-

gotiate QUIC with clients or not. Can specify one of NONE, ENABLE, or DISABLE. If NONE is specified, uses the QUIC policy with no user overrides, which is equivalent to DISABLE. Not specifying this field is equivalent to specifying NONE.

- **ssl\_policy** - (Optional) A reference to the SslPolicy resource that will be associated with the TargetHttpsProxy resource. If not set, the TargetHttpsProxy resource will not have any SSL policy configured.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **proxy\_id** - The unique identifier for the resource.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

TargetHttpsProxy can be imported using any of these accepted formats:

```
$ terraform import google_compute_target_https_proxy.default projects/{{project}}/global/targetHttpsProxies/{{name}}
$ terraform import google_compute_target_https_proxy.default {{project}}/{{name}}
$ terraform import google_compute_target_https_proxy.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_target\_ssl\_proxy

Represents a TargetSslProxy resource, which is used by one or more global forwarding rule to route incoming SSL requests to a backend service.

To get more information about TargetSslProxy, see:

- API documentation
- How-to Guides
  - Setting Up SSL proxy for Google Cloud Load Balancing



OPEN IN GOOGLE CLOUD SHELL

### » Example Usage - Target Ssl Proxy Basic

```
resource "google_compute_target_ssl_proxy" "default" {
  name          = "test-proxy"
  backend_service = "${google_compute_backend_service.default.self_link}"
  ssl_certificates = ["${google_compute_ssl_certificate.default.self_link}"]
}

resource "google_compute_ssl_certificate" "default" {
  name          = "default-cert"
  private_key   = "${file("path/to/private.key")}"
  certificate   = "${file("path/to/certificate.crt")}"
}

resource "google_compute_backend_service" "default" {
  name          = "backend-service"
  protocol      = "SSL"
  health_checks = ["${google_compute_health_check.default.self_link}"]
}

resource "google_compute_health_check" "default" {
  name          = "health-check"
  check_interval_sec = 1
  timeout_sec    = 1
  tcp_health_check {
    port = "443"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- **backend\_service** - (Required) A reference to the BackendService resource.
- **ssl\_certificates** - (Required) A list of SslCertificate resources that are used to authenticate connections between users and the load balancer. Currently, exactly one SSL certificate must be specified.

- 
- **description** - (Optional) An optional description of this resource.
  - **proxy\_header** - (Optional) Specifies the type of proxy header to append before sending data to the backend, either NONE or PROXY\_V1. The default is NONE.
  - **ssl\_policy** - (Optional) A reference to the SslPolicy resource that will be associated with the TargetSslProxy resource. If not set, the TargetSslProxy resource will not have any SSL policy configured.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **proxy\_id** - The unique identifier for the resource.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.

- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

TargetSslProxy can be imported using any of these accepted formats:

```
$ terraform import google_compute_target_ssl_proxy.default projects/{{project}}/global/targetSslProxy/{{name}}
$ terraform import google_compute_target_ssl_proxy.default {{project}}/{{name}}
$ terraform import google_compute_target_ssl_proxy.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_compute_target_tcp_proxy`

Represents a TargetTcpProxy resource, which is used by one or more global forwarding rule to route incoming TCP requests to a Backend service.

To get more information about TargetTcpProxy, see:

- API documentation
- How-to Guides
  - Setting Up TCP proxy for Google Cloud Load Balancing



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Target Tcp Proxy Basic

```
resource "google_compute_target_tcp_proxy" "default" {
  name          = "test-proxy"
  backend_service = "${google_compute_backend_service.default.self_link}"
}

resource "google_compute_backend_service" "default" {
  name          = "backend-service"
  protocol      = "TCP"
  timeout_sec   = 10

  health_checks = ["${google_compute_health_check.default.self_link}"]
}
```



```

}

resource "google_compute_health_check" "default" {
  name           = "health-check"
  timeout_sec    = 1
  check_interval_sec = 1

  tcp_health_check {
    port = "443"
  }
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
  - **backend\_service** - (Required) A reference to the BackendService resource.
- 
- **description** - (Optional) An optional description of this resource.
  - **proxy\_header** - (Optional) Specifies the type of proxy header to append before sending data to the backend, either NONE or PROXY\_V1. The default is NONE.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **proxy\_id** - The unique identifier for the resource.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

TargetTcpProxy can be imported using any of these accepted formats:

```
$ terraform import google_compute_target_tcp_proxy.default projects/{{project}}/global/targetTcpProxies/{{name}}
$ terraform import google_compute_target_tcp_proxy.default {{project}}/{{name}}
$ terraform import google_compute_target_tcp_proxy.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_target\_pool

Manages a Target Pool within GCE. This is a collection of instances used as target of a network load balancer (Forwarding Rule). For more information see the official documentation and API.

## » Example Usage

```
resource "google_compute_target_pool" "default" {
  name = "instance-pool"

  instances = [
    "us-central1-a/myinstance1",
    "us-central1-b/myinstance2",
  ]

  health_checks = [
    "${google_compute_http_health_check.default.name}",
  ]
}

resource "google_compute_http_health_check" "default" {
  name          = "default"
  request_path  = "/"
}
```

```

    check_interval_sec = 1
    timeout_sec        = 1
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique name for the resource, required by GCE. Changing this forces a new resource to be created.
- 
- **backup\_pool** - (Optional) URL to the backup target pool. Must also set `failover_ratio`.
  - **description** - (Optional) Textual description field.
  - **failover\_ratio** - (Optional) Ratio (0 to 1) of failed nodes before using the backup pool (which must also be set).
  - **health\_checks** - (Optional) List of zero or one health check name or `self_link`. Only legacy `google_compute_http_health_check` is supported.
  - **instances** - (Optional) List of instances in the pool. They can be given as URLs, or in the form of "zone/name". Note that the instances need not exist at the time of target pool creation, so there is no need to use the Terraform interpolators to create a dependency on the instances from the target pool.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
  - **region** - (Optional) Where the target pool resides. Defaults to project region.
  - **session\_affinity** - (Optional) How to distribute load. Options are "NONE" (no affinity), "CLIENT\_IP" (hash of the source/dest addresses / ports), and "CLIENT\_IP\_PROTO" also includes the protocol (default "NONE").

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **self\_link** - The URI of the created resource.

## » Import

Target pools can be imported using the `name`, e.g.

```
$ terraform import google_compute_target_pool.default instance-pool
```

## » google\_\_compute\_\_url\_\_map

UrlMaps are used to route requests to a backend service based on rules that you define for the host and path of an incoming URL.



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Url Map Basic

```
resource "google_compute_url_map" "urlmap" {
  name          = "urlmap"
  description   = "a description"

  default_service = "${google_compute_backend_service.home.self_link}"

  host_rule {
    hosts          = ["mysite.com"]
    path_matcher   = "allpaths"
  }

  path_matcher {
    name           = "allpaths"
    default_service = "${google_compute_backend_service.home.self_link}"

    path_rule {
      paths      = ["/home"]
      service    = "${google_compute_backend_service.home.self_link}"
    }

    path_rule {
      paths      = ["/login"]
      service    = "${google_compute_backend_service.login.self_link}"
    }
  }
}
```

```

    path_rule {
      paths    = ["/static"]
      service = "${google_compute_backend_bucket.static.self_link}"
    }
  }

  test {
    service = "${google_compute_backend_service.home.self_link}"
    host    = "hi.com"
    path    = "/home"
  }
}

resource "google_compute_backend_service" "login" {
  name          = "login"
  port_name     = "http"
  protocol      = "HTTP"
  timeout_sec   = 10

  health_checks = ["${google_compute_http_health_check.default.self_link}"]
}

resource "google_compute_backend_service" "home" {
  name          = "home"
  port_name     = "http"
  protocol      = "HTTP"
  timeout_sec   = 10

  health_checks = ["${google_compute_http_health_check.default.self_link}"]
}

resource "google_compute_http_health_check" "default" {
  name          = "health-check"
  request_path   = "/"
  check_interval_sec = 1
  timeout_sec    = 1
}

resource "google_compute_backend_bucket" "static" {
  name          = "static-asset-backend-bucket"
  bucket_name   = "${google_storage_bucket.static.name}"
  enable_cdn    = true
}

resource "google_storage_bucket" "static" {
  name = "static-asset-bucket"
}

```

```

    location = "US"
}

```

## » Argument Reference

The following arguments are supported:

- **default\_service** - (Required) The backend service or backend bucket to use when none of the given rules match.
  - **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- 
- **description** - (Optional) An optional description of this resource. Provide this property when you create the resource.
  - **host\_rule** - (Optional) The list of HostRules to use against the URL. Structure is documented below.
  - **path\_matcher** - (Optional) The list of named PathMatchers to use against the URL. Structure is documented below.
  - **test** - (Optional) The list of expected URL mappings. Requests to update this UrlMap will succeed only if all of the test cases pass. Structure is documented below.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **host\_rule** block supports:

- **description** - (Optional) An optional description of this HostRule. Provide this property when you create the resource.
- **hosts** - (Required) The list of host patterns to match. They must be valid hostnames, except `*` will match any string of `([a-z0-9-]*)`. In that case, `*` must be the first character and must be followed in the pattern by either `-` or `..`.
- **path\_matcher** - (Required) The name of the PathMatcher to use to match the path portion of the URL if the hostRule matches the URL's host portion.

The **path\_matcher** block supports:

- **default\_service** - (Required) The backend service or backend bucket to use when none of the given paths match.
- **description** - (Optional) An optional description of this resource.
- **name** - (Required) The name to which this PathMatcher is referred by the HostRule.
- **path\_rule** - (Optional) The list of path rules. Structure is documented below.

The **path\_rule** block supports:

- **paths** - (Required) The list of path patterns to match. Each must start with / and the only place a \* is allowed is at the end following a /. The string fed to the path matcher does not include any text after the first ? or #, and those chars are not allowed here.
- **service** - (Required) The backend service or backend bucket to use if any of the given paths match.

The **test** block supports:

- **description** - (Optional) Description of this test case.
- **host** - (Required) Host portion of the URL.
- **path** - (Required) Path portion of the URL.
- **service** - (Required) The backend service or backend bucket link that should be matched by this test.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **map\_id** - The unique identifier for the resource.
- **fingerprint** - Fingerprint of this resource. This field is used internally during updates of this resource.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.

- delete - Default is 4 minutes.

## » Import

UrlMap can be imported using any of these accepted formats:

```
$ terraform import google_compute_url_map.default projects/{{project}}/global/urlMaps/{{name}}
$ terraform import google_compute_url_map.default {{project}}/{{name}}
$ terraform import google_compute_url_map.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_compute\_vpn\_gateway

Represents a VPN gateway running in GCP. This virtual device is managed by Google, but used only by you.

To get more information about VpnGateway, see:

- [API documentation](#)



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Target Vpn Gateway Basic

```
resource "google_compute_vpn_gateway" "target_gateway" {
  name      = "vpn1"
  network   = "${google_compute_network.network1.self_link}"
}

resource "google_compute_network" "network1" {
  name      = "network1"
}

resource "google_compute_address" "vpn_static_ip" {
  name      = "vpn-static-ip"
}

resource "google_compute_forwarding_rule" "fr_esp" {
```



```

    name          = "fr-esp"
    ip_protocol    = "ESP"
    ip_address     = "${google_compute_address.vpn_static_ip.address}"
    target         = "${google_compute_vpn_gateway.target_gateway.self_link}"
  }

  resource "google_compute_forwarding_rule" "fr_udp500" {
    name          = "fr-udp500"
    ip_protocol    = "UDP"
    port_range     = "500"
    ip_address     = "${google_compute_address.vpn_static_ip.address}"
    target         = "${google_compute_vpn_gateway.target_gateway.self_link}"
  }

  resource "google_compute_forwarding_rule" "fr_udp4500" {
    name          = "fr-udp4500"
    ip_protocol    = "UDP"
    port_range     = "4500"
    ip_address     = "${google_compute_address.vpn_static_ip.address}"
    target         = "${google_compute_vpn_gateway.target_gateway.self_link}"
  }

  resource "google_compute_vpn_tunnel" "tunnel1" {
    name          = "tunnel1"
    peer_ip       = "15.0.0.120"
    shared_secret = "a secret message"

    target_vpn_gateway = "${google_compute_vpn_gateway.target_gateway.self_link}"

    depends_on = [
      "google_compute_forwarding_rule.fr_esp",
      "google_compute_forwarding_rule.fr_udp500",
      "google_compute_forwarding_rule.fr_udp4500",
    ]
  }

  resource "google_compute_route" "route1" {
    name          = "route1"
    network       = "${google_compute_network.network1.name}"
    dest_range    = "15.0.0.0/24"
    priority      = 1000

    next_hop_vpn_tunnel = "${google_compute_vpn_tunnel.tunnel1.self_link}"
  }

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. Provided by the client when the resource is created. The name must be 1-63 characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.
- **network** - (Required) The network this VPN gateway is accepting traffic for.

- 
- **description** - (Optional) An optional description of this resource.
  - **region** - (Optional) The region this gateway should sit in.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **self\_link** - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

VpnGateway can be imported using any of these accepted formats:

```
$ terraform import google_compute_vpn_gateway.default projects/{{project}}/regions/{{region}}/{{name}}
$ terraform import google_compute_vpn_gateway.default {{project}}/{{region}}/{{name}}
$ terraform import google_compute_vpn_gateway.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_compute_vpn_tunnel`

VPN tunnel resource.

To get more information about `VpnTunnel`, see:

- API documentation
- How-to Guides
  - Cloud VPN Overview
  - Networks and Tunnel Routing

**Warning:** All arguments including the shared secret will be stored in the raw state as plain-text. Read more about sensitive data in state.



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Vpn Tunnel Basic

```
resource "google_compute_vpn_tunnel" "tunnel1" {
  name           = "tunnel1"
  peer_ip        = "15.0.0.120"
  shared_secret  = "a secret message"

  target_vpn_gateway = "${google_compute_vpn_gateway.target_gateway.self_link}"

  depends_on = [
    "google_compute_forwarding_rule.fr_esp",
    "google_compute_forwarding_rule.fr_udp500",
    "google_compute_forwarding_rule.fr_udp4500",
  ]
}

resource "google_compute_vpn_gateway" "target_gateway" {
  name     = "vpn1"
  network  = "${google_compute_network.network1.self_link}"
}
```

```

resource "google_compute_network" "network1" {
  name      = "network1"
}

resource "google_compute_address" "vpn_static_ip" {
  name      = "vpn-static-ip"
}

resource "google_compute_forwarding_rule" "fr_esp" {
  name          = "fr-esp"
  ip_protocol   = "ESP"
  ip_address    = "${google_compute_address.vpn_static_ip.address}"
  target        = "${google_compute_vpn_gateway.target_gateway.self_link}"
}

resource "google_compute_forwarding_rule" "fr_udp500" {
  name          = "fr-udp500"
  ip_protocol   = "UDP"
  port_range    = "500"
  ip_address    = "${google_compute_address.vpn_static_ip.address}"
  target        = "${google_compute_vpn_gateway.target_gateway.self_link}"
}

resource "google_compute_forwarding_rule" "fr_udp4500" {
  name          = "fr-udp4500"
  ip_protocol   = "UDP"
  port_range    = "4500"
  ip_address    = "${google_compute_address.vpn_static_ip.address}"
  target        = "${google_compute_vpn_gateway.target_gateway.self_link}"
}

resource "google_compute_route" "route1" {
  name          = "route1"
  network       = "${google_compute_network.network1.name}"
  dest_range    = "15.0.0.0/24"
  priority      = 1000

  next_hop_vpn_tunnel = "${google_compute_vpn_tunnel.tunnel1.self_link}"
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the resource. The name must be 1-63

characters long, and comply with RFC1035. Specifically, the name must be 1-63 characters long and match the regular expression `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

- **target\_vpn\_gateway** - (Required) URL of the Target VPN gateway with which this VPN tunnel is associated.
- **peer\_ip** - (Required) IP address of the peer VPN gateway. Only IPv4 is supported.
- **shared\_secret** - (Required) Shared secret used to set the secure session between the Cloud VPN gateway and the peer VPN gateway.

- 
- **description** - (Optional) An optional description of this resource.
  - **router** - (Optional) URL of router resource to be used for dynamic routing.
  - **ike\_version** - (Optional) IKE protocol version to use when establishing the VPN tunnel with peer VPN gateway. Acceptable IKE versions are 1 or 2. Default version is 2.
  - **local\_traffic\_selector** - (Optional) Local traffic selector to use when establishing the VPN tunnel with peer VPN gateway. The value should be a CIDR formatted string, for example `192.168.0.0/16`. The ranges should be disjoint. Only IPv4 is supported.
  - **remote\_traffic\_selector** - (Optional) Remote traffic selector to use when establishing the VPN tunnel with peer VPN gateway. The value should be a CIDR formatted string, for example `192.168.0.0/16`. The ranges should be disjoint. Only IPv4 is supported.
  - **labels** - (Optional) Labels to apply to this VpnTunnel.
  - **region** - (Optional) The region where the tunnel is located. If unset, is set to the region of **target\_vpn\_gateway**.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **creation\_timestamp** - Creation timestamp in RFC3339 text format.
- **shared\_secret\_hash** - Hash of the shared secret.

- `label_fingerprint` - The fingerprint used for optimistic locking of this resource. Used internally during updates.
- `detailed_status` - Detailed status message for the VPN tunnel.
- `self_link` - The URI of the created resource.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

VpnTunnel can be imported using any of these accepted formats:

```
$ terraform import google_compute_vpn_tunnel.default projects/{{project}}/regions/{{region}}/{{name}}
$ terraform import google_compute_vpn_tunnel.default {{project}}/{{region}}/{{name}}
$ terraform import google_compute_vpn_tunnel.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_container\_\_analysis\_\_note

Provides a detailed description of a Note.

**Warning:** This resource is in beta, and should be used with the `terraform-provider-google-beta` provider. See [Provider Versions](#) for more details on beta resources.

To get more information about Note, see:

- [API documentation](#)
- [How-to Guides](#)
  - [Official Documentation](#)



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Container Analysis Note Basic

```
resource "google_container_analysis_note" "note" {
  provider = "google-beta"

  name = "test-attestor-note"
  attestation_authority {
    hint {
      human_readable_name = "Attestor Note"
    }
  }
}

provider "google-beta" {
  region = "us-central1"
  zone   = "us-central1-a"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the note.
- **attestation\_authority** - (Required) Note kind that represents a logical attestation "role" or "authority". For example, an organization might have one AttestationAuthority for "QA" and one for "build". This Note is intended to act strictly as a grouping mechanism for the attached Occurrences (Attestations). This grouping mechanism also provides a security boundary, since IAM ACLs gate the ability for a principle to attach an Occurrence to a given Note. It also provides a single point of lookup to find all attached Attestation Occurrences, even if they don't all live in the same project. Structure is documented below.

The **attestation\_authority** block supports:

- **hint** - (Required) This submessage provides human-readable hints about the purpose of the AttestationAuthority. Because the name of a Note acts as its resource reference, it is important to disambiguate the canonical name of the Note (which might be a UUID for security purposes) from "readable" names more suitable for debug output. Note that these hints should NOT be used to look up AttestationAuthorities in security sensitive contexts, such as when looking up Attestations to verify. Structure is documented below.

The **hint** block supports:

- `human_readable_name` - (Required) The human readable name of this Attestation Authority, for example "qa".

- 
- `project` - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Note can be imported using any of these accepted formats:

```
$ terraform import -provider=google-beta google_container_analysis_note.default projects/{{project}}/{{name}}
$ terraform import -provider=google-beta google_container_analysis_note.default {{project}}/{{name}}
$ terraform import -provider=google-beta google_container_analysis_note.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_container\_\_cluster

Manages a Google Kubernetes Engine (GKE) cluster. For more information see the official documentation and the API reference.

**Note:** All arguments and attributes, including basic auth username and passwords as well as certificate outputs will be stored in the raw state as plaintext. Read more about sensitive data in state.

## » Example Usage - with a separately managed node pool (recommended)

```
resource "google_container_cluster" "primary" {
  name     = "my-gke-cluster"
  region   = "us-central1"
```



```

# We can't create a cluster with no node pool defined, but we want to only use
# separately managed node pools. So we create the smallest possible default
# node pool and immediately delete it.
remove_default_node_pool = true
initial_node_count = 1

# Setting an empty username and password explicitly disables basic auth
master_auth {
  username = ""
  password = ""
}

node_config {
  oauth_scopes = [
    "https://www.googleapis.com/auth/compute",
    "https://www.googleapis.com/auth/devstorage.read_only",
    "https://www.googleapis.com/auth/logging.write",
    "https://www.googleapis.com/auth/monitoring",
  ]

  labels = {
    foo = "bar"
  }

  tags = ["foo", "bar"]
}
}

resource "google_container_node_pool" "primary_preemptible_nodes" {
  name      = "my-node-pool"
  region    = "us-central1"
  cluster   = "${google_container_cluster.primary.name}"
  node_count = 1

  node_config {
    preemptible = true
    machine_type = "n1-standard-1"

    oauth_scopes = [
      "https://www.googleapis.com/auth/compute",
      "https://www.googleapis.com/auth/devstorage.read_only",
      "https://www.googleapis.com/auth/logging.write",
      "https://www.googleapis.com/auth/monitoring",
    ]
  }
}
}

```

```

# The following outputs allow authentication and connectivity to the GKE Cluster
# by using certificate-based authentication.
output "client_certificate" {
  value = "${google_container_cluster.primary.master_auth.0.client_certificate}"
}

output "client_key" {
  value = "${google_container_cluster.primary.master_auth.0.client_key}"
}

output "cluster_ca_certificate" {
  value = "${google_container_cluster.primary.master_auth.0.cluster_ca_certificate}"
}

```

## » Example Usage - with the default node pool

```

resource "google_container_cluster" "primary" {
  name          = "marcellus-wallace"
  zone          = "us-central1-a"
  initial_node_count = 3

  # Setting an empty username and password explicitly disables basic auth
  master_auth {
    username = ""
    password = ""
  }

  node_config {
    oauth_scopes = [
      "https://www.googleapis.com/auth/compute",
      "https://www.googleapis.com/auth/devstorage.read_only",
      "https://www.googleapis.com/auth/logging.write",
      "https://www.googleapis.com/auth/monitoring",
    ]

    labels = {
      foo = "bar"
    }

    tags = ["foo", "bar"]
  }

  timeouts {
    create = "30m"
  }
}

```

```

        update = "40m"
    }
}

# The following outputs allow authentication and connectivity to the GKE Cluster
# by using certificate-based authentication.
output "client_certificate" {
    value = "${google_container_cluster.primary.master_auth.0.client_certificate}"
}

output "client_key" {
    value = "${google_container_cluster.primary.master_auth.0.client_key}"
}

output "cluster_ca_certificate" {
    value = "${google_container_cluster.primary.master_auth.0.cluster_ca_certificate}"
}

```

## » Argument Reference

- **name** - (Required) The name of the cluster, unique within the project and zone.
- 
- **zone** - (Optional) The zone that the master and the number of nodes specified in **initial\_node\_count** should be created in. Only one of **zone** and **region** may be set. If neither zone nor region are set, the provider zone is used.
  - **region** (Optional) The region to create the cluster in for Regional Clusters. In a Regional Cluster, the number of nodes specified in **initial\_node\_count** is created in each of three zones of the region (this can be changed by setting **additional\_zones**).
  - **additional\_zones** - (Optional) The list of additional Google Compute Engine locations in which the cluster's nodes should be located. If additional zones are configured, the number of nodes specified in **initial\_node\_count** is created in all specified zones.
  - **addons\_config** - (Optional) The configuration for addons supported by GKE. Structure is documented below.
  - **cluster\_ipv4\_cidr** - (Optional) The IP address range of the kubernetes pods in this cluster. Default is an automatically assigned CIDR.
  - **cluster\_autoscaling** - (Optional, Beta) Configuration for cluster autoscaling (also called autoprovisioning), as described in the docs. Struc-

ture is documented below.

- **description** - (Optional) Description of the cluster.
- **enable\_binary\_authorization** - (Optional, Beta) Enable Binary Authorization for this cluster. If enabled, all container images will be validated by Google Binary Authorization.
- **enable\_kubernetes\_alpha** - (Optional) Whether to enable Kubernetes Alpha features for this cluster. Note that when this option is enabled, the cluster cannot be upgraded and will be automatically deleted after 30 days.
- **enable\_tpu** - (Optional, Beta) Whether to enable Cloud TPU resources in this cluster. See the official documentation.
- **enable\_legacy\_abac** - (Optional) Whether the ABAC authorizer is enabled for this cluster. When enabled, identities in the system, including service accounts, nodes, and controllers, will have statically granted permissions beyond those provided by the RBAC configuration or IAM. Defaults to **false**
- **initial\_node\_count** - (Optional) The number of nodes to create in this cluster (not including the Kubernetes master). Must be set if **node\_pool** is not set.
- **ip\_allocation\_policy** - (Optional) Configuration for cluster IP allocation. As of now, only pre-allocated subnetworks (custom type with secondary ranges) are supported. This will activate IP aliases. See the official documentation Structure is documented below.
- **logging\_service** - (Optional) The logging service that the cluster should write logs to. Available options include **logging.googleapis.com**, **logging.googleapis.com/kubernetes** (beta), and **none**. Defaults to **logging.googleapis.com**
- **maintenance\_policy** - (Optional) The maintenance policy to use for the cluster. Structure is documented below.
- **master\_auth** - (Optional) The authentication information for accessing the Kubernetes master. Structure is documented below.
- **master\_authorized\_networks\_config** - (Optional) The desired configuration options for master authorized networks. Omit the nested **cidr\_blocks** attribute to disallow external access (except the cluster node IPs, which GKE automatically whitelists).
- **min\_master\_version** - (Optional) The minimum version of the master. GKE will auto-update the master to new versions, so this does not guarantee the current master version--use the read-only **master\_version** field to obtain that. If unset, the cluster's version will be set by GKE to the version of the most recent official release (which is not necessarily the latest

version). Most users will find the `google_container_engine_versions` data source useful - it indicates which versions are available, and can be used to approximate fuzzy versions in a Terraform-compatible way. If you intend to specify versions manually, the docs describe the various acceptable formats for this field.

If you are using the `google_container_engine_versions` datasource with a regional cluster, ensure that you have provided a `region` to the datasource. A `region` can have a different set of supported versions than its corresponding `zones`, and not all `zones` in a `region` are guaranteed to support the same version.

- `monitoring_service` - (Optional) The monitoring service that the cluster should write metrics to. Automatically send metrics from pods in the cluster to the Google Cloud Monitoring API. VM metrics will be collected by Google Compute Engine regardless of this setting. Available options include `monitoring.googleapis.com`, `monitoring.googleapis.com/kubernetes` (beta) and `none`. Defaults to `monitoring.googleapis.com`
- `network` - (Optional) The name or `self_link` of the Google Compute Engine network to which the cluster is connected. For Shared VPC, set this to the self link of the shared network.
- `network_policy` - (Optional) Configuration options for the NetworkPolicy feature. Structure is documented below.
- `node_config` - (Optional) Parameters used in creating the cluster's nodes. Structure is documented below.
- `node_pool` - (Optional) List of node pools associated with this cluster. See `google_container_node_pool` for schema. **Warning:** node pools defined inside a cluster can't be changed (or added/removed) after cluster creation without deleting and recreating the entire cluster. Unless you absolutely need the ability to say "these are the *only* node pools associated with this cluster", use the `google_container_node_pool` resource instead of this property.
- `node_version` - (Optional) The Kubernetes version on the nodes. Must either be unset or set to the same value as `min_master_version` on create. Defaults to the default version set by GKE which is not necessarily the latest version. This only affects nodes in the default node pool. While a fuzzy version can be specified, it's recommended that you specify explicit versions as Terraform will see spurious diffs when fuzzy versions are used. See the `google_container_engine_versions` data source's `version_prefix` field to approximate fuzzy versions in a Terraform-compatible way. To update nodes in other node pools, use the `version` attribute on the node pool.
- `pod_security_policy_config` - (Optional, Beta) Configuration for the PodSecurityPolicy feature. Structure is documented below.

- **private\_cluster\_config** - (Optional) A set of options for creating a private cluster. Structure is documented below.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **remove\_default\_node\_pool** - (Optional) If true, deletes the default node pool upon cluster creation.
- **resource\_labels** - (Optional) The GCE resource labels (a map of key/value pairs) to be applied to the cluster.
- **subnetwork** - (Optional) The name or self\_link of the Google Compute Engine subnetwork in which the cluster's instances are launched.

The **addons\_config** block supports:

- **horizontal\_pod\_autoscaling** - (Optional) The status of the Horizontal Pod Autoscaling addon, which increases or decreases the number of replica pods a replication controller has based on the resource usage of the existing pods. It ensures that a Heapster pod is running in the cluster, which is also used by the Cloud Monitoring service. It is enabled by default; set **disabled = true** to disable.
- **http\_load\_balancing** - (Optional) The status of the HTTP (L7) load balancing controller addon, which makes it easy to set up HTTP load balancers for services in a cluster. It is enabled by default; set **disabled = true** to disable.
- **kubernetes\_dashboard** - (Optional) The status of the Kubernetes Dashboard add-on, which controls whether the Kubernetes Dashboard is enabled for this cluster. It is enabled by default; set **disabled = true** to disable.
- **network\_policy\_config** - (Optional) Whether we should enable the network policy addon for the master. This must be enabled in order to enable network policy for the nodes. It can only be disabled if the nodes already do not have network policies enabled. Defaults to disabled; set **disabled = false** to enable.
- **istio\_config** - (Optional, Beta). Structure is documented below.
- **cloudrun\_config** - (Optional, Beta). The status of the CloudRun addon. It requires **istio\_config** enabled. It is disabled by default. Set **disabled = false** to enable. This addon can only be enabled at cluster creation time.

This example **addons\_config** disables two addons:

```
addons_config {
  http_load_balancing {
    disabled = true
```

```

    }
    horizontal_pod_autoscaling {
        disabled = true
    }
}

```

The `istio_config` block supports: \* `disabled` - (Optional) The status of the Istio addon, which makes it easy to set up Istio for services in a cluster. It is disabled by default. Set `disabled = false` to enable. \* `auth` - (Optional) The authentication type between services in Istio. Available options include `AUTH_MUTUAL_TLS`.

The `cluster_autoscaling` block supports: \* `enabled` - (Required) Whether cluster autoscaling (also called autoprovisioning) is enabled. To set this to true, make sure your config meets the rest of the requirements. Notably, you'll need `min_master_version` of at least 1.11.2. \* `resource_limits` - (Optional) A list of limits on the autoprovisioning. See the docs for an explanation of what options are available. If enabling autoprovisioning, make sure to set at least `cpu` and `memory`. Structure is documented below.

The `resource_limits` block supports:

- `resource_type` - (Required) See the docs for a list of permitted types - `cpu`, `memory`, and others.
- `minimum` - (Optional) The minimum value for the resource type specified.
- `maximum` - (Optional) The maximum value for the resource type specified.

The `maintenance_policy` block supports:

- `daily_maintenance_window` - (Required) Time window specified for daily maintenance operations. Specify `start_time` in RFC3339 format "HH:MM", where HH : [00-23] and MM : [00-59] GMT. For example:

```

maintenance_policy {
    daily_maintenance_window {
        start_time = "03:00"
    }
}

```

The `ip_allocation_policy` block supports:

- `use_ip_aliases` - (Optional) Whether alias IPs will be used for pod IPs in the cluster. Defaults to `true` if the `ip_allocation_policy` block is defined, and to the API default otherwise. Prior to June 17th 2019, the default on the API is `false`; afterwards, it's `true`.
- `cluster_secondary_range_name` - (Optional) The name of the secondary range to be used as for the cluster CIDR block. The secondary range will be used for pod IP addresses. This must be an existing secondary range associated with the cluster subnetwork.

- **services\_secondary\_range\_name** - (Optional) The name of the secondary range to be used as for the services CIDR block. The secondary range will be used for service ClusterIPs. This must be an existing secondary range associated with the cluster subnetwork.
- **cluster\_ipv4\_cidr\_block** - (Optional) The IP address range for the cluster pod IPs. Set to blank to have a range chosen with the default size. Set to /netmask (e.g. /14) to have a range chosen with a specific netmask. Set to a CIDR notation (e.g. 10.96.0.0/14) from the RFC-1918 private networks (e.g. 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) to pick a specific range to use.
- **node\_ipv4\_cidr\_block** - (Optional) The IP address range of the node IPs in this cluster. Set to blank to have a range chosen with the default size. Set to /netmask (e.g. /14) to have a range chosen with a specific netmask. Set to a CIDR notation (e.g. 10.96.0.0/14) from the RFC-1918 private networks (e.g. 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) to pick a specific range to use.
- **services\_ipv4\_cidr\_block** - (Optional) The IP address range of the services IPs in this cluster. Set to blank to have a range chosen with the default size. Set to /netmask (e.g. /14) to have a range chosen with a specific netmask. Set to a CIDR notation (e.g. 10.96.0.0/14) from the RFC-1918 private networks (e.g. 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) to pick a specific range to use.
- **create\_subnetwork**- (Optional) Whether a new subnetwork will be created automatically for the cluster.
- **subnetwork\_name** - (Optional) A custom subnetwork name to be used if create\_subnetwork is true. If this field is empty, then an automatic name will be chosen for the new subnetwork.

The **master\_auth** block supports:

- **password** - (Optional) The password to use for HTTP basic authentication when accessing the Kubernetes master endpoint.
- **username** - (Optional) The username to use for HTTP basic authentication when accessing the Kubernetes master endpoint. If not present basic auth will be disabled.
- **client\_certificate\_config** - (Optional) Whether client certificate authorization is enabled for this cluster. For example:

```
master_auth {
  client_certificate_config {
    issue_client_certificate = false
  }
}
```



If this block is provided and both `username` and `password` are empty, basic authentication will be disabled. This block also contains several computed attributes, documented below. If this block is not provided, GKE will generate a password for you with the username `admin`.

The `master_authorized_networks_config` block supports:

- `cidr_blocks` - (Optional) Defines up to 20 external networks that can access Kubernetes master through HTTPS.

The `master_authorized_networks_config.cidr_blocks` block supports:

- `cidr_block` - (Optional) External network that can access Kubernetes master through HTTPS. Must be specified in CIDR notation.
- `display_name` - (Optional) Field for users to identify CIDR blocks.

The `network_policy` block supports:

- `provider` - (Optional) The selected network policy provider. Defaults to `PROVIDER_UNSPECIFIED`.
- `enabled` - (Optional) Whether network policy is enabled on the cluster. Defaults to false.

The `node_config` block supports:

- `disk_size_gb` - (Optional) Size of the disk attached to each node, specified in GB. The smallest allowed disk size is 10GB. Defaults to 100GB.
- `disk_type` - (Optional) Type of the disk attached to each node (e.g. 'pd-standard' or 'pd-ssd'). If unspecified, the default disk type is 'pd-standard'.
- `guest_accelerator` - (Optional) List of the type and count of accelerator cards attached to the instance. Structure documented below.
- `image_type` - (Optional) The image type to use for this node. Note that changing the image type will delete and recreate all nodes in the node pool.
- `labels` - (Optional) The Kubernetes labels (key/value pairs) to be applied to each node.
- `local_ssd_count` - (Optional) The amount of local SSD disks that will be attached to each cluster node. Defaults to 0.
- `machine_type` - (Optional) The name of a Google Compute Engine machine type. Defaults to `n1-standard-1`. To create a custom machine type, value should be set as specified here.
- `metadata` - (Optional) The metadata key/value pairs assigned to instances in the cluster.
- `min_cpu_platform` - (Optional) Minimum CPU platform to be used by this instance. The instance may be scheduled on the specified or newer

CPU platform. Applicable values are the friendly names of CPU platforms, such as `Intel Haswell`. See the official documentation for more information.

- **oauth\_scopes** - (Optional) The set of Google API scopes to be made available on all of the node VMs under the "default" service account. These can be either FQDNs, or scope aliases. The following scopes are necessary to ensure the correct functioning of the cluster:
  - `compute-rw` (<https://www.googleapis.com/auth/compute>)
  - `storage-ro` ([https://www.googleapis.com/auth/devstorage.read\\_only](https://www.googleapis.com/auth/devstorage.read_only))
  - `logging-write` (<https://www.googleapis.com/auth/logging.write>), if `logging_service` points to Google
  - `monitoring` (<https://www.googleapis.com/auth/monitoring>), if `monitoring_service` points to Google
- **preemptible** - (Optional) A boolean that represents whether or not the underlying node VMs are preemptible. See the official documentation for more information. Defaults to false.
- **service\_account** - (Optional) The service account to be used by the Node VMs. If not specified, the "default" service account is used. In order to use the configured **oauth\_scopes** for logging and monitoring, the service account being used needs the `roles/logging.logWriter` and `roles/monitoring.metricWriter` roles.

Projects that enable the Cloud Compute Engine API with Terraform may need these roles added manually to the service account. Projects that enable the API in the Cloud Console should have them added automatically.

- **tags** - (Optional) The list of instance tags applied to all nodes. Tags are used to identify valid sources or targets for network firewalls.
- **taint** - (Optional, Beta) List of kubernetes taints to apply to each node. Structure is documented below.
- **workload\_metadata\_config** - (Optional, Beta) Metadata configuration to expose to workloads on the node pool. Structure is documented below.

The **guest\_accelerator** block supports:

- **type** (Required) - The accelerator type resource to expose to this instance. E.g. `nvidia-tesla-k80`.
- **count** (Required) - The number of the guest accelerator cards exposed to this instance.

The **pod\_security\_policy\_config** block supports:

- **enabled** (Required) - Enable the PodSecurityPolicy controller for this cluster. If enabled, pods must be valid under a PodSecurityPolicy to be created.

The `private_cluster_config` block supports:

- `enable_private_endpoint` (Optional) - Whether the master's internal IP address is used as the cluster endpoint.
- `enable_private_nodes` (Optional) - Whether nodes have internal IP addresses only. If enabled, all nodes are given only RFC 1918 private addresses and communicate with the master via private networking.
- `master_ipv4_cidr_block` (Optional) - The IP range in CIDR notation to use for the hosted master network. This range will be used for assigning internal IP addresses to the master or set of masters, as well as the ILB VIP. This range must not overlap with any other ranges in use within the cluster's network.

In addition, the `private_cluster_config` allows access to the following read-only fields:

- `private_endpoint` - The internal IP address of this cluster's master endpoint.
- `public_endpoint` - The external IP address of this cluster's master endpoint.

The `taint` block supports:

- `key` (Required) Key for taint.
- `value` (Required) Value for taint.
- `effect` (Required) Effect for taint. Accepted values are `NO_SCHEDULE`, `PREFER_NO_SCHEDULE`, and `NO_EXECUTE`.

The `workload_metadata_config` block supports:

- `node_metadata` (Required) How to expose the node metadata to the workload running on the node. Accepted values are:
  - `UNSPECIFIED`: Not Set
  - `SECURE`: Prevent workloads not in `hostNetwork` from accessing certain VM metadata, specifically `kube-env`, which contains Kubelet credentials, and the instance identity token. See Metadata Concealment documentation.
  - `EXPOSE`: Expose all VM metadata to pods.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `endpoint` - The IP address of this cluster's Kubernetes master.

- `instance_group_urls` - List of instance group URLs which have been assigned to the cluster.
- `maintenance_policy.0.daily_maintenance_window.0.duration` - Duration of the time window, automatically chosen to be smallest possible in the given scenario. Duration will be in RFC3339 format "PTnHnMnS".
- `master_auth.0.client_certificate` - Base64 encoded public certificate used by clients to authenticate to the cluster endpoint.
- `master_auth.0.client_key` - Base64 encoded private key used by clients to authenticate to the cluster endpoint.
- `master_auth.0.cluster_ca_certificate` - Base64 encoded public certificate that is the root of trust for the cluster.
- `master_version` - The current version of the master in the cluster. This may be different than the `min_master_version` set in the config if the master has been updated by GKE.
- `tpu_ipv4_cidr_block` - (Beta) The IP address range of the Cloud TPUs in this cluster, in CIDR notation (e.g. 1.2.3.4/29).

## » Timeouts

`google_container_cluster` provides the following Timeouts configuration options:

- `create` - (Default 30 minutes) Used for clusters
- `update` - (Default 30 minutes) Used for updates to clusters
- `delete` - (Default 30 minutes) Used for destroying clusters.

## » Import

GKE clusters can be imported using the `project`, `zone` or `region`, and `name`. If the project is omitted, the default provider value will be used. Examples:

```
$ terraform import google_container_cluster.mycluster my-gcp-project/us-east1-a/my-cluster
```

```
$ terraform import google_container_cluster.mycluster us-east1-a/my-cluster
```

**Note:** This resource has several fields that control Terraform-specific behavior and aren't present in the API. If they are set in config and you import a cluster, Terraform may need to perform an update immediately after import. Most of these updates should be no-ops but some may modify your cluster if the imported state differs.

For example, the following fields will show diffs if set in config:

- min\_master\_version
- remove\_default\_node\_pool

## » google\_\_container\_\_node\_\_pool

Manages a node pool in a Google Kubernetes Engine (GKE) cluster separately from the cluster control plane. For more information see the official documentation and the API reference.

» **Example Usage - using a separately managed node pool (recommended)**

```
resource "google_container_cluster" "primary" {
  name     = "my-gke-cluster"
  region   = "us-central1"

  # We can't create a cluster with no node pool defined, but we want to only use
  # separately managed node pools. So we create the smallest possible default
  # node pool and immediately delete it.
  remove_default_node_pool = true
  initial_node_count = 1
}

resource "google_container_node_pool" "primary_preemptible_nodes" {
  name           = "my-node-pool"
  region         = "us-central1"
  cluster        = "${google_container_cluster.primary.name}"
  node_count     = 1

  node_config {
    preemptible  = true
    machine_type = "n1-standard-1"

    oauth_scopes = [
      "https://www.googleapis.com/auth/compute",
      "https://www.googleapis.com/auth/devstorage.read_only",
      "https://www.googleapis.com/auth/logging.write",
      "https://www.googleapis.com/auth/monitoring",
    ]
  }
}
```

» Example Usage - 2 node pools, 1 separately managed + the default node pool

```
resource "google_container_node_pool" "np" {
  name      = "my-node-pool"
  zone      = "us-central1-a"
  cluster   = "${google_container_cluster.primary.name}"
  node_count = 3

  timeouts {
    create = "30m"
    update = "20m"
  }
}

resource "google_container_cluster" "primary" {
  name          = "marcellus-wallace"
  zone          = "us-central1-a"
  initial_node_count = 3

  additional_zones = [
    "us-central1-c",
  ]

  # Setting an empty username and password explicitly disables basic auth
  master_auth {
    username = ""
    password = ""
  }

  node_config {
    oauth_scopes = [
      "https://www.googleapis.com/auth/compute",
      "https://www.googleapis.com/auth/devstorage.read_only",
      "https://www.googleapis.com/auth/logging.write",
      "https://www.googleapis.com/auth/monitoring",
    ]

    guest_accelerator {
      type  = "nvidia-tesla-k80"
      count = 1
    }
  }
}
```

## » Argument Reference

- **cluster** - (Required) The cluster to create the node pool for. Cluster must be present in **zone** provided for zonal clusters.

- 
- **zone** - (Optional) The zone in which the cluster resides.
  - **region** - (Optional) The region in which the cluster resides (for regional clusters).

Note: You must be provide **region** for regional clusters and **zone** for zonal clusters

- 
- **autoscaling** - (Optional) Configuration required by cluster autoscaler to adjust the size of the node pool to the current cluster usage. Structure is documented below.
  - **initial\_node\_count** - (Optional) The initial node count for the pool. Changing this will force recreation of the resource.
  - **management** - (Optional) Node management configuration, wherein auto-repair and auto-upgrade is configured. Structure is documented below.
  - **max\_pods\_per\_node** - (Optional, Beta) The maximum number of pods per node in this node pool. Note that this does not work on node pools which are "route-based" - that is, node pools belonging to clusters that do not have IP Aliasing enabled.
  - **name** - (Optional) The name of the node pool. If left blank, Terraform will auto-generate a unique name.
  - **node\_config** - (Optional) The node configuration of the pool. See `google_container_cluster` for schema.
  - **node\_count** - (Optional) The number of nodes per instance group. This field can be used to update the number of nodes per instance group but should not be used alongside **autoscaling**.
  - **project** - (Optional) The ID of the project in which to create the node pool. If blank, the provider-configured project will be used.
  - **version** - (Optional) The Kubernetes version for the nodes in this pool. Note that if this field and **auto\_upgrade** are both specified, they will fight each other for what the node version should be, so setting both is highly discouraged. While a fuzzy version can be specified, it's recommended that you specify explicit versions as Terraform will see spurious diffs when fuzzy versions are used. See the `google_container_engine_versions`

data source's `version_prefix` field to approximate fuzzy versions in a Terraform-compatible way.

The `autoscaling` block supports:

- `min_node_count` - (Required) Minimum number of nodes in the NodePool. Must be  $\geq 0$  and  $\leq \text{max\_node\_count}$ .
- `max_node_count` - (Required) Maximum number of nodes in the NodePool. Must be  $\geq \text{min\_node\_count}$ .

The `management` block supports:

- `auto_repair` - (Optional) Whether the nodes will be automatically repaired.
- `auto_upgrade` - (Optional) Whether the nodes will be automatically upgraded.

## » Timeouts

`google_container_node_pool` provides the following Timeouts configuration options:

- `create` - (Default 30 minutes) Used for adding node pools
- `update` - (Default 10 minutes) Used for updates to node pools
- `delete` - (Default 10 minutes) Used for removing node pools.

## » Import

Node pools can be imported using the `project`, `zone`, `cluster` and `name`. If the project is omitted, the default provider value will be used. Examples:

```
$ terraform import google_container_node_pool.mainpool my-gcp-project/us-east1-a/my-cluster
```

```
$ terraform import google_container_node_pool.mainpool us-east1-a/my-cluster/main-pool
```

## » google\_\_dataflow\_\_job

Creates a job on Dataflow, which is an implementation of Apache Beam running on Google Compute Engine. For more information see the official documentation for Beam and Dataflow.



## » Example Usage

```
resource "google_dataflow_job" "big_data_job" {
  name = "dataflow-job"
  template_gcs_path = "gs://my-bucket/templates/template_file"
  temp_gcs_location = "gs://my-bucket/tmp_dir"
  parameters = {
    foo = "bar"
    baz = "qux"
  }
}
```

## » Note on "destroy" / "apply"

There are many types of Dataflow jobs. Some Dataflow jobs run constantly, getting new data from (e.g.) a GCS bucket, and outputting data continuously. Some jobs process a set amount of data then terminate. All jobs can fail while running due to programming errors or other issues. In this way, Dataflow jobs are different from most other Terraform / Google resources.

The Dataflow resource is considered 'existing' while it is in a nonterminal state. If it reaches a terminal state (e.g. 'FAILED', 'COMPLETE', 'CANCELLED'), it will be recreated on the next 'apply'. This is as expected for jobs which run continuously, but may surprise users who use this resource for other kinds of Dataflow jobs.

A Dataflow job which is 'destroyed' may be "cancelled" or "drained". If "cancelled", the job terminates - any data written remains where it is, but no new data will be processed. If "drained", no new data will enter the pipeline, but any data currently in the pipeline will finish being processed. The default is "cancelled", but if a user sets `on_delete` to "drain" in the configuration, you may experience a long wait for your `terraform destroy` to complete.

## » Argument Reference

The following arguments are supported:

- `name` - (Required) A unique name for the resource, required by Dataflow.
- `template_gcs_path` - (Required) The GCS path to the Dataflow job template.
- `temp_gcs_location` - (Required) A writeable location on GCS for the Dataflow job to dump its temporary data.

- **parameters** - (Optional) Key/Value pairs to be passed to the Dataflow job (as used in the template).
- **max\_workers** - (Optional) The number of workers permitted to work on the job. More workers may improve processing speed at additional cost.
- **on\_delete** - (Optional) One of "drain" or "cancel". Specifies behavior of deletion during **terraform destroy**. See above note.
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
- **zone** - (Optional) The zone in which the created job should run. If it is not provided, the provider zone is used.

## » Attributes Reference

- **state** - The current state of the resource, selected from the JobState enum

## » google\_dataproc\_cluster

Manages a Cloud Dataproc cluster resource within GCP. For more information see the official dataproc documentation.

**Warning:** Due to limitations of the API, all arguments except `labels`, `cluster_config.worker_config.num_instances` and `cluster_config.preemptible_worker_config.num_instances` are non-updateable. Changing others will cause recreation of the whole cluster!

## » Example Usage - Basic

```
resource "google_dataproc_cluster" "simplecluster" {
  name     = "simplecluster"
  region   = "us-central1"
}
```

## » Example Usage - Advanced

```
resource "google_dataproc_cluster" "mycluster" {
  name     = "mycluster"
  region   = "us-central1"
  labels = {
    foo = "bar"
  }

  cluster_config {
    staging_bucket = "dataproc-staging-bucket"
  }
}
```

```

master_config {
  num_instances      = 1
  machine_type       = "n1-standard-1"
  disk_config {
    boot_disk_type = "pd-ssd"
    boot_disk_size_gb = 15
  }
}

worker_config {
  num_instances      = 2
  machine_type       = "n1-standard-1"
  disk_config {
    boot_disk_size_gb = 15
    num_local_ssds    = 1
  }
}

preemptible_worker_config {
  num_instances      = 0
}

# Override or set some custom properties
software_config {
  image_version      = "1.3.7-deb9"
  override_properties = {
    "dataproc:dataproc.allow.zero.workers" = "true"
  }
}

gce_cluster_config {
  #network = "${google_compute_network.dataproc_network.name}"
  tags     = ["foo", "bar"]
}

# You can define multiple initialization_action blocks
initialization_action {
  script      = "gs://dataproc-initialization-actions/stackdriver/stackdriver.sh"
  timeout_sec = 500
}

}
}

```

## » Example Usage - Using a GPU accelerator

```
resource "google_dataproc_cluster" "accelerated_cluster" {
  name     = "my-cluster-with-gpu"
  region   = "us-central1"

  cluster_config {
    gce_cluster_config {
      zone = "us-central1-a"
    }

    master_config {
      accelerators {
        accelerator_type = "nvidia-tesla-k80"
        accelerator_count = "1"
      }
    }
  }
}
```

## » Argument Reference

- **name** - (Required) The name of the cluster, unique within the project and zone.
- 
- **project** - (Optional) The ID of the project in which the `cluster` will exist. If it is not provided, the provider project is used.
  - **region** - (Optional) The region in which the cluster and associated nodes will be created in. Defaults to `global`.
  - **labels** - (Optional, Computed) The list of labels (key/value pairs) to be applied to instances in the cluster. GCP generates some itself including `goog-dataproc-cluster-name` which is the name of the cluster.
  - **cluster\_config** - (Optional) Allows you to configure various aspects of the cluster. Structure defined below.
- 

The `cluster_config` block supports:

```
cluster_config {
  gce_cluster_config      { ... }
  master_config           { ... }
  worker_config           { ... }
  preemptible_worker_config { ... }
```

```

software_config          { ... }

# You can define multiple initialization_action blocks
initialization_action    { ... }
encryption_config        { ... }
}

```

- **staging\_bucket** - (Optional) The Cloud Storage staging bucket used to stage files, such as Hadoop jars, between client machines and the cluster. Note: If you don't explicitly specify a **staging\_bucket** then GCP will auto create / assign one for you. However, you are not guaranteed an auto generated bucket which is solely dedicated to your cluster; it may be shared with other clusters in the same region/zone also choosing to use the auto generation option.
- **gce\_cluster\_config** (Optional) Common config settings for resources of Google Compute Engine cluster instances, applicable to all instances in the cluster. Structure defined below.
- **master\_config** (Optional) The Google Compute Engine config settings for the master instances in a cluster.. Structure defined below.
- **worker\_config** (Optional) The Google Compute Engine config settings for the worker instances in a cluster.. Structure defined below.
- **preemptible\_worker\_config** (Optional) The Google Compute Engine config settings for the additional (aka preemptible) instances in a cluster. Structure defined below.
- **software\_config** (Optional) The config settings for software inside the cluster. Structure defined below.
- **initialization\_action** (Optional) Commands to execute on each node after config is completed. You can specify multiple versions of these. Structure defined below.
- **encryption\_config** (Optional) The Customer managed encryption keys settings for the cluster. Structure defined below.

---

The `cluster_config.gce_cluster_config` block supports:

```

cluster_config {
  gce_cluster_config {

    zone = "us-central1-a"

    # One of the below to hook into a custom network / subnetwork
    network      = "${google_compute_network.dataproc_network.name}"
    subnetwork    = "${google_compute_network.dataproc_subnetwork.name}"
  }
}

```

```

        tags    = ["foo", "bar"]
    }
}

```

- **zone** - (Optional, Computed) The GCP zone where your data is stored and used (i.e. where the master and the worker nodes will be created in). If **region** is set to 'global' (default) then **zone** is mandatory, otherwise GCP is able to make use of Auto Zone Placement to determine this automatically for you. Note: This setting additionally determines and restricts which computing resources are available for use with other configs such as `cluster_config.master_config.machine_type` and `cluster_config.worker_config.machine_type`.
- **network** - (Optional, Computed) The name or self\_link of the Google Compute Engine network to the cluster will be part of. Conflicts with **subnetwork**. If neither is specified, this defaults to the "default" network.
- **subnetwork** - (Optional) The name or self\_link of the Google Compute Engine subnetwork the cluster will be part of. Conflicts with **network**.
- **service\_account** - (Optional) The service account to be used by the Node VMs. If not specified, the "default" service account is used.
- **service\_account\_scopes** - (Optional, Computed) The set of Google API scopes to be made available on all of the node VMs under the **service\_account** specified. These can be either FQDNs, or scope aliases. The following scopes are necessary to ensure the correct functioning of the cluster:
  - `useraccounts-ro` (<https://www.googleapis.com/auth/cloud.useraccounts.readonly>)
  - `storage-rw` ([https://www.googleapis.com/auth/devstorage.read\\_write](https://www.googleapis.com/auth/devstorage.read_write))
  - `logging-write` (<https://www.googleapis.com/auth/logging.write>)
- **tags** - (Optional) The list of instance tags applied to instances in the cluster. Tags are used to identify valid sources or targets for network firewalls.
- **internal\_ip\_only** - (Optional) By default, clusters are not restricted to internal IP addresses, and will have ephemeral external IP addresses assigned to each instance. If set to true, all instances in the cluster will only have internal IP addresses. Note: Private Google Access (also known as `privateIpGoogleAccess`) must be enabled on the subnetwork that the cluster will be launched in.
- **metadata** - (Optional) A map of the Compute Engine metadata entries to add to all instances (see Project and instance metadata).

---

The `cluster_config.master_config` block supports:

```

cluster_config {
  master_config {
    num_instances      = 1
    machine_type       = "n1-standard-1"
    disk_config {
      boot_disk_type   = "pd-ssd"
      boot_disk_size_gb = 15
      num_local_ssds   = 1
    }
  }
}

```

- **num\_instances**- (Optional, Computed) Specifies the number of master nodes to create. If not specified, GCP will default to a predetermined computed value (currently 1).
- **machine\_type** - (Optional, Computed) The name of a Google Compute Engine machine type to create for the master. If not specified, GCP will default to a predetermined computed value (currently **n1-standard-4**).
- **image\_uri** (Optional) The URI for the image to use for this worker. See the guide for more information.
- **disk\_config** (Optional) Disk Config
  - **boot\_disk\_type** - (Optional) The disk type of the primary disk attached to each node. One of "**pd-ssd**" or "**pd-standard**". Defaults to "**pd-standard**".
  - **boot\_disk\_size\_gb** - (Optional, Computed) Size of the primary disk attached to each node, specified in GB. The primary disk contains the boot volume and system libraries, and the smallest allowed disk size is 10GB. GCP will default to a predetermined computed value if not set (currently 500GB). Note: If SSDs are not attached, it also contains the HDFS data blocks and Hadoop working directories.
  - **num\_local\_ssds** - (Optional) The amount of local SSD disks that will be attached to each master cluster node. Defaults to 0.
- **accelerators** (Optional) The Compute Engine accelerator (GPU) configuration for these instances. Can be specified multiple times.
  - **accelerator\_type** - (Required) The short name of the accelerator type to expose to this instance. For example, **nvidia-tesla-k80**.
  - **accelerator\_count** - (Required) The number of the accelerator cards of this type exposed to this instance. Often restricted to one of 1, 2, 4, or 8.

The Cloud Dataproc API can return unintuitive error messages when using accelerators; even when you have defined an accelerator, Auto Zone Placement does not exclusively select zones that have that accelerator available. If you get a 400 error that the accelerator can't be found, this is a likely cause. Make sure

you check accelerator availability by zone if you are trying to use accelerators in a given zone.

---

The `cluster_config.worker_config` block supports:

```
cluster_config {
  worker_config {
    num_instances      = 3
    machine_type       = "n1-standard-1"
    disk_config {
      boot_disk_type   = "pd-standard"
      boot_disk_size_gb = 15
      num_local_ssds   = 1
    }
  }
}
```

- **num\_instances**- (Optional, Computed) Specifies the number of worker nodes to create. If not specified, GCP will default to a predetermined computed value (currently 2). There is currently a beta feature which allows you to run a Single Node Cluster. In order to take advantage of this you need to set `"dataproc:dataproc.allow.zero.workers" = "true"` in `cluster_config.software_config.properties`
- **machine\_type** - (Optional, Computed) The name of a Google Compute Engine machine type to create for the worker nodes. If not specified, GCP will default to a predetermined computed value (currently `n1-standard-4`).
- **disk\_config** (Optional) Disk Config
  - **boot\_disk\_type** - (Optional) The disk type of the primary disk attached to each node. One of `"pd-ssd"` or `"pd-standard"`. Defaults to `"pd-standard"`.
  - **boot\_disk\_size\_gb** - (Optional, Computed) Size of the primary disk attached to each worker node, specified in GB. The smallest allowed disk size is 10GB. GCP will default to a predetermined computed value if not set (currently 500GB). Note: If SSDs are not attached, it also contains the HDFS data blocks and Hadoop working directories.
  - **num\_local\_ssds** - (Optional) The amount of local SSD disks that will be attached to each worker cluster node. Defaults to 0.
- **image\_uri** (Optional) The URI for the image to use for this worker. See the guide for more information.
- **accelerators** (Optional) The Compute Engine accelerator configuration for these instances. Can be specified multiple times.



- **accelerator\_type** - (Required) The short name of the accelerator type to expose to this instance. For example, `nvidia-tesla-k80`.
- **accelerator\_count** - (Required) The number of the accelerator cards of this type exposed to this instance. Often restricted to one of 1, 2, 4, or 8.

The Cloud Dataproc API can return unintuitive error messages when using accelerators; even when you have defined an accelerator, Auto Zone Placement does not exclusively select zones that have that accelerator available. If you get a 400 error that the accelerator can't be found, this is a likely cause. Make sure you check accelerator availability by zone if you are trying to use accelerators in a given zone.

---

The `cluster_config.preemptible_worker_config` block supports:

```
cluster_config {
  preemptible_worker_config {
    num_instances      = 1
    disk_config {
      boot_disk_type   = "pd-standard"
      boot_disk_size_gb = 15
      num_local_ssds   = 1
    }
  }
}
```

Note: Unlike `worker_config`, you cannot set the `machine_type` value directly. This will be set for you based on whatever was set for the `worker_config.machine_type` value.

- **num\_instances**- (Optional) Specifies the number of preemptible nodes to create. Defaults to 0.
- **disk\_config** (Optional) Disk Config
  - **boot\_disk\_type** - (Optional) The disk type of the primary disk attached to each preemptible worker node. One of `"pd-ssd"` or `"pd-standard"`. Defaults to `"pd-standard"`.
  - **boot\_disk\_size\_gb** - (Optional, Computed) Size of the primary disk attached to each preemptible worker node, specified in GB. The smallest allowed disk size is 10GB. GCP will default to a predetermined computed value if not set (currently 500GB). Note: If SSDs are not attached, it also contains the HDFS data blocks and Hadoop working directories.
  - **num\_local\_ssds** - (Optional) The amount of local SSD disks that will be attached to each preemptible worker node. Defaults to 0.

The `cluster_config.software_config` block supports:

```
cluster_config {
  # Override or set some custom properties
  software_config {
    image_version      = "1.3.7-deb9"
    override_properties = {
      "dataproc:dataproc.allow.zero.workers" = "true"
    }
  }
}
```

- `image_version` - (Optional, Computed) The Cloud Dataproc image version to use for the cluster - this controls the sets of software versions installed onto the nodes when you create clusters. If not specified, defaults to the latest version. For a list of valid versions see Cloud Dataproc versions
- `override_properties` - (Optional) A list of override and additional properties (key/value pairs) used to modify various aspects of the common configuration files used when creating a cluster. For a list of valid properties please see Cluster properties

---

The `initialization_action` block (Optional) can be specified multiple times and supports:

```
cluster_config {
  # You can define multiple initialization_action blocks
  initialization_action {
    script      = "gs://dataproc-initialization-actions/stackdriver/stackdriver.sh"
    timeout_sec = 500
  }
}
```

- `script` - (Required) The script to be executed during initialization of the cluster. The script must be a GCS file with a `gs://` prefix.
- `timeout_sec` - (Optional, Computed) The maximum duration (in seconds) which `script` is allowed to take to execute its action. GCP will default to a predetermined computed value if not set (currently 300).

---

The `encryption_config` block supports:

```
cluster_config {
  encryption_config {
    kms_key_name = "projects/projectId/locations/region/keyRings/keyRingName/cryptob"
  }
}
```

```

    }
  }

```

- **kms\_key\_name** - (Required) The Cloud KMS key name to use for PD disk encryption for all instances in the cluster.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **cluster\_config.0.master\_config.0.instance\_names** - List of master instance names which have been assigned to the cluster.
- **cluster\_config.0.worker\_config.0.instance\_names** - List of worker instance names which have been assigned to the cluster.
- **cluster\_config.0.preemptible\_worker\_config.0.instance\_names** - List of preemptible instance names which have been assigned to the cluster.
- **cluster\_config.0.bucket** - The name of the cloud storage bucket ultimately used to house the staging data for the cluster. If **staging\_bucket** is specified, it will contain this value, otherwise it will be the auto generated name.
- **cluster\_config.0.software\_config.0.properties** - A list of the properties used to set the daemon config files. This will include any values supplied by the user via **cluster\_config.software\_config.override\_properties**

## » Timeouts

**google\_dataproc\_cluster** provides the following Timeouts configuration options:

- **create** - (Default 10 minutes) Used for creating clusters.
- **update** - (Default 5 minutes) Used for updating clusters
- **delete** - (Default 5 minutes) Used for destroying clusters.

## » google\_\_dataproc\_\_job

Manages a job resource within a Dataproc cluster within GCE. For more information see the official dataproc documentation.

**Note:** This resource does not support 'update' and changing any attributes will cause the resource to be recreated.

## » Example usage

```
resource "google_dataproc_cluster" "mycluster" {
  name     = "dproc-cluster-unique-name"
  region   = "us-central1"
}

# Submit an example spark job to a dataproc cluster
resource "google_dataproc_job" "spark" {
  region      = "${google_dataproc_cluster.mycluster.region}"
  force_delete = true
  placement {
    cluster_name = "${google_dataproc_cluster.mycluster.name}"
  }

  spark_config {
    main_class      = "org.apache.spark.examples.SparkPi"
    jar_file_uris   = ["file:///usr/lib/spark/examples/jars/spark-examples.jar"]
    args            = ["1000"]

    properties      = {
      "spark.logConf" = "true"
    }

    logging_config {
      driver_log_levels = {
        "root" = "INFO"
      }
    }
  }
}

# Submit an example pyspark job to a dataproc cluster
resource "google_dataproc_job" "pyspark" {
  region      = "${google_dataproc_cluster.mycluster.region}"
  force_delete = true
  placement {
    cluster_name = "${google_dataproc_cluster.mycluster.name}"
  }

  pyspark_config {
    main_python_file_uri = "gs://dataproc-examples-2f10d78d114f6aaec76462e3c310f31f/src/
    properties = {
      "spark.logConf" = "true"
    }
  }
}
```

```

    }
}

# Check out current state of the jobs
output "spark_status" {
    value = "${google_dataproc_job.spark.status.0.state}"
}

output "pyspark_status" {
    value = "${google_dataproc_job.pyspark.status.0.state}"
}

```

## » Argument Reference

- `placement.cluster_name` - (Required) The name of the cluster where the job will be submitted.
  - `xxx_config` - (Required) Exactly one of the specific job types to run on the cluster should be specified. If you want to submit multiple jobs, this will currently require the definition of multiple `google_dataproc_job` resources as shown in the example above, or by setting the `count` attribute. The following job configs are supported:
    - `pyspark_config` - Submits a PySpark job to the cluster
    - `spark_config` - Submits a Spark job to the cluster
    - `hadoop_config` - Submits a Hadoop job to the cluster
    - `hive_config` - Submits a Hive job to the cluster
    - `hpig_config` - Submits a Pig job to the cluster
    - `sparksql_config` - Submits a Spark SQL job to the cluster
- 
- `project` - (Optional) The project in which the `cluster` can be found and jobs subsequently run against. If it is not provided, the provider project is used.
  - `region` - (Optional) The Cloud Dataproc region. This essentially determines which clusters are available for this job to be submitted to. If not specified, defaults to `global`.
  - `force_delete` - (Optional) By default, you can only delete inactive jobs within Dataproc. Setting this to true, and calling `destroy`, will ensure that the job is first cancelled before issuing the delete.
  - `labels` - (Optional) The list of labels (key/value pairs) to add to the job.
  - `scheduling.max_failures_per_hour` - (Optional) Maximum number of times per hour a driver may be restarted as a result of driver terminating with non-zero code before job is reported failed.

The `pyspark_config` block supports:

Submitting a pyspark job to the cluster. Below is an example configuration:

```
# Submit a pyspark job to the cluster
resource "google_dataproc_job" "pyspark" {
  ...

  pyspark_config {
    main_python_file_uri = "gs://dataproc-examples-2f10d78d114f6aaec76462e3c310f31f/src/
    properties = {
      "spark.logConf" = "true"
    }
  }
}
```

For configurations requiring Hadoop Compatible File System (HCFS) references, the options below are generally applicable:

- GCS files with the ``gs://`` prefix
- HDFS files on the cluster with the ``hdfs://`` prefix
- Local files on the cluster with the ``file://`` prefix
- `main_python_file_uri`- (Required) The HCFS URI of the main Python file to use as the driver. Must be a .py file.
- `args` - (Optional) The arguments to pass to the driver.
- `python_file_uris` - (Optional) HCFS file URIs of Python files to pass to the PySpark framework. Supported file types: .py, .egg, and .zip.
- `jar_file_uris` - (Optional) HCFS URIs of jar files to add to the CLASSPATHs of the Python driver and tasks.
- `file_uris` - (Optional) HCFS URIs of files to be copied to the working directory of Python drivers and distributed tasks. Useful for naively parallel tasks.
- `archive_uris` - (Optional) HCFS URIs of archives to be extracted in the working directory of .jar, .tar, .tar.gz, .tgz, and .zip.
- `properties` - (Optional) A mapping of property names to values, used to configure PySpark. Properties that conflict with values set by the Cloud Dataproc API may be overwritten. Can include properties set in `/etc/spark/conf/spark-defaults.conf` and classes in user code.
- `logging_config.driver_log_levels`- (Optional) The per-package log levels for the driver. This may include 'root' package name to configure rootLogger. Examples: `'com.google = FATAL'`, `'root = INFO'`, `'org.apache = DEBUG'`

The `spark_config` block supports:

```

# Submit a spark job to the cluster
resource "google_dataproc_job" "spark" {
  ...

  spark_config {
    main_class      = "org.apache.spark.examples.SparkPi"
    jar_file_uris   = ["file:///usr/lib/spark/examples/jars/spark-examples.jar"]
    args            = ["1000"]

    properties      = {
      "spark.logConf" = "true"
    }

    logging_config {
      driver_log_levels = {
        "root" = "INFO"
      }
    }
  }
}

```

- **main\_class**- (Optional) The class containing the main method of the driver. Must be in a provided jar or jar that is already on the classpath. Conflicts with **main\_jar\_file\_uri**
- **main\_jar\_file\_uri** - (Optional) The HCFS URI of jar file containing the driver jar. Conflicts with **main\_class**
- **args** - (Optional) The arguments to pass to the driver.
- **jar\_file\_uris** - (Optional) HCFS URIs of jar files to add to the CLASSPATHs of the Spark driver and tasks.
- **file\_uris** - (Optional) HCFS URIs of files to be copied to the working directory of Spark drivers and distributed tasks. Useful for naively parallel tasks.
- **archive\_uris** - (Optional) HCFS URIs of archives to be extracted in the working directory of .jar, .tar, .tar.gz, .tgz, and .zip.
- **properties** - (Optional) A mapping of property names to values, used to configure Spark. Properties that conflict with values set by the Cloud Dataproc API may be overwritten. Can include properties set in `/etc/spark/conf/spark-defaults.conf` and classes in user code.
- **logging\_config.driver\_log\_levels**- (Optional) The per-package log levels for the driver. This may include 'root' package name to configure rootLogger. Examples: 'com.google = FATAL', 'root = INFO', 'org.apache = DEBUG'

The `hadoop_config` block supports:

```
# Submit a hadoop job to the cluster
resource "google_dataproc_job" "hadoop" {
  ...

  hadoop_config {
    main_jar_file_uri = "file:///usr/lib/hadoop-mapreduce/hadoop-mapreduce-examples.jar"
    args              = [
      "wordcount",
      "file:///usr/lib/spark/NOTICE",
      "gs://${google_dataproc_cluster.basic.cluster_config.0.bucket}/hadoopjob_output"
    ]
  }
}
```

- **main\_class**- (Optional) The name of the driver's main class. The jar file containing the class must be in the default CLASSPATH or specified in `jar_file_uris`. Conflicts with `main_jar_file_uri`
- **main\_jar\_file\_uri** - (Optional) The HCFS URI of the jar file containing the main class. Examples: 'gs://foo-bucket/analytics-binaries/extract-useful-metrics-mr.jar' 'hdfs://tmp/test-samples/custom-wordcount.jar' 'file:///home/usr/lib/hadoop-mapreduce/hadoop-mapreduce-examples.jar'. Conflicts with `main_class`
- **args** - (Optional) The arguments to pass to the driver. Do not include arguments, such as `-libjars` or `-Dfoo=bar`, that can be set as job properties, since a collision may occur that causes an incorrect job submission.
- **jar\_file\_uris** - (Optional) HCFS URIs of jar files to add to the CLASSPATHs of the Spark driver and tasks.
- **file\_uris** - (Optional) HCFS URIs of files to be copied to the working directory of Hadoop drivers and distributed tasks. Useful for naively parallel tasks.
- **archive\_uris** - (Optional) HCFS URIs of archives to be extracted in the working directory of `.jar`, `.tar`, `.tar.gz`, `.tgz`, and `.zip`.
- **properties** - (Optional) A mapping of property names to values, used to configure Hadoop. Properties that conflict with values set by the Cloud Dataproc API may be overwritten. Can include properties set in `/etc/hadoop/conf/*-site` and classes in user code..
- **logging\_config.driver\_log\_levels**- (Optional) The per-package log levels for the driver. This may include 'root' package name to configure rootLogger. Examples: 'com.google = FATAL', 'root = INFO', 'org.apache = DEBUG'

The `hive_config` block supports:



```

# Submit a hive job to the cluster
resource "google_dataproc_job" "hive" {
  ...

  hive_config {
    query_list = [
      "DROP TABLE IF EXISTS dprocjob_test",
      "CREATE EXTERNAL TABLE dprocjob_test(bar int) LOCATION 'gs://${google_dataproc_
      "SELECT * FROM dprocjob_test WHERE bar > 2",
    ]
  }
}

```

- **query\_list**- (Optional) The list of Hive queries or statements to execute as part of the job. Conflicts with **query\_file\_uri**
- **query\_file\_uri** - (Optional) HCFS URI of file containing Hive script to execute as the job. Conflicts with **query\_list**
- **continue\_on\_failure** - (Optional) Whether to continue executing queries if a query fails. The default value is false. Setting to true can be useful when executing independent parallel queries. Defaults to false.
- **script\_variables** - (Optional) Mapping of query variable names to values (equivalent to the Hive command: **SET name="value";**).
- **properties** - (Optional) A mapping of property names and values, used to configure Hive. Properties that conflict with values set by the Cloud Dataproc API may be overwritten. Can include properties set in `/etc/hadoop/conf/*-site.xml`, `/etc/hive/conf/hive-site.xml`, and classes in user code..
- **jar\_file\_uris** - (Optional) HCFS URIs of jar files to add to the CLASSPATH of the Hive server and Hadoop MapReduce (MR) tasks. Can contain Hive SerDes and UDFs.

The **pig\_config** block supports:

```

# Submit a pig job to the cluster
resource "google_dataproc_job" "pig" {
  ...

  pig_config {
    query_list = [
      "LNS = LOAD 'file:///usr/lib/pig/LICENSE.txt ' AS (line)",
      "WORDS = FOREACH LNS GENERATE FLATTEN(TOKENIZE(line)) AS word",
      "GROUPS = GROUP WORDS BY word",
      "WORD_COUNTS = FOREACH GROUPS GENERATE group, COUNT(WORDS)",
      "DUMP WORD_COUNTS"
    ]
  }
}

```

```

    }
}

```

- **query\_list**- (Optional) The list of Hive queries or statements to execute as part of the job. Conflicts with **query\_file\_uri**
- **query\_file\_uri** - (Optional) HCFS URI of file containing Hive script to execute as the job. Conflicts with **query\_list**
- **continue\_on\_failure** - (Optional) Whether to continue executing queries if a query fails. The default value is false. Setting to true can be useful when executing independent parallel queries. Defaults to false.
- **script\_variables** - (Optional) Mapping of query variable names to values (equivalent to the Pig command: **name=[value]**).
- **properties** - (Optional) A mapping of property names to values, used to configure Pig. Properties that conflict with values set by the Cloud Dataproc API may be overwritten. Can include properties set in `/etc/hadoop/conf/*-site.xml`, `/etc/pig/conf/pig.properties`, and classes in user code.
- **jar\_file\_uris** - (Optional) HCFS URIs of jar files to add to the CLASSPATH of the Pig Client and Hadoop MapReduce (MR) tasks. Can contain Pig UDFs.
- **logging\_config.driver\_log\_levels**- (Optional) The per-package log levels for the driver. This may include 'root' package name to configure rootLogger. Examples: 'com.google = FATAL', 'root = INFO', 'org.apache = DEBUG'

The **sparksql\_config** block supports:

```

# Submit a spark SQL job to the cluster
resource "google_dataproc_job" "sparksql" {
  ...

  sparksql_config {
    query_list = [
      "DROP TABLE IF EXISTS dprocjob_test",
      "CREATE TABLE dprocjob_test(bar int)",
      "SELECT * FROM dprocjob_test WHERE bar > 2",
    ]
  }
}

```

- **query\_list**- (Optional) The list of SQL queries or statements to execute as part of the job. Conflicts with **query\_file\_uri**
- **query\_file\_uri** - (Optional) The HCFS URI of the script that contains SQL queries. Conflicts with **query\_list**

- **script\_variables** - (Optional) Mapping of query variable names to values (equivalent to the Spark SQL command: `SET name="value";`).
- **properties** - (Optional) A mapping of property names to values, used to configure Spark SQL's SparkConf. Properties that conflict with values set by the Cloud Dataproc API may be overwritten.
- **jar\_file\_uris** - (Optional) HCFS URIs of jar files to be added to the Spark CLASSPATH.
- **logging\_config.driver\_log\_levels** - (Optional) The per-package log levels for the driver. This may include 'root' package name to configure rootLogger. Examples: 'com.google = FATAL', 'root = INFO', 'org.apache = DEBUG'

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **reference.0.cluster\_uuid** - A cluster UUID generated by the Cloud Dataproc service when the job is submitted.
- **status.0.state** - A state message specifying the overall job state.
- **status.0.details** - Optional job state details, such as an error description if the state is ERROR.
- **status.0.state\_start\_time** - The time when this state was entered.
- **status.0.substate** - Additional state information, which includes status reported by the agent.
- **driver\_output\_resource\_uri** - A URI pointing to the location of the stdout of the job's driver program.
- **driver\_controls\_files\_uri** - If present, the location of miscellaneous control files which may be used as part of job setup and handling. If not present, control files may be placed in the same location as `driver_output_uri`.

## » Timeouts

`google_dataproc_cluster` provides the following Timeouts configuration options:

- **create** - (Default 10 minutes) Used for submitting a job to a dataproc cluster.

- `delete` - (Default 10 minutes) Used for deleting a job from a dataproc cluster.

## » `google__dns__managed__zone`

A zone is a subtree of the DNS namespace under one administrative responsibility. A ManagedZone is a resource that represents a DNS zone hosted by the Cloud DNS service.

To get more information about ManagedZone, see:

- API documentation
- How-to Guides
  - Managing Zones



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Dns Managed Zone Basic

```
resource "google_dns_managed_zone" "example-zone" {
  name = "example-zone"
  dns_name = "example-${random_id.rnd.hex}.com."
  description = "Example DNS zone"
  labels = {
    foo = "bar"
  }
}

resource "random_id" "rnd" {
  byte_length = 4
}
```

## » Example Usage - Dns Managed Zone Private

```
resource "google_dns_managed_zone" "private-zone" {
  name = "private-zone"
  dns_name = "private.example.com."
  description = "Example private DNS zone"
  labels = {
    foo = "bar"
  }
}
```

```

}

visibility = "private"

private_visibility_config {
  networks {
    network_url = "${google_compute_network.network-1.self_link}"
  }
  networks {
    network_url = "${google_compute_network.network-2.self_link}"
  }
}

forwarding_config {
  target_name_servers {
    ipv4_address = "172.16.1.10"
  }
  target_name_servers {
    ipv4_address = "172.16.1.20"
  }
}
}

resource "google_compute_network" "network-1" {
  name = "network-1"
  auto_create_subnetworks = false
}

resource "google_compute_network" "network-2" {
  name = "network-2"
  auto_create_subnetworks = false
}

```

## » Argument Reference

The following arguments are supported:

- **dns\_name** - (Required) The DNS name of this managed zone, for instance "example.com".
- **name** - (Required) User assigned name for this resource. Must be unique within the project.

- **description** - (Optional) A textual description field. Defaults to 'Managed by Terraform'.
- **labels** - (Optional) A set of key/value label pairs to assign to this ManagedZone.
- **visibility** - (Optional, Beta) The zone's visibility: public zones are exposed to the Internet, while private zones are visible only to Virtual Private Cloud resources. Must be one of: **public**, **private**.
- **private\_visibility\_config** - (Optional, Beta) For privately visible zones, the set of Virtual Private Cloud resources that the zone is visible from. Structure is documented below.
- **forwarding\_config** - (Optional, Beta) The presence for this field indicates that outbound forwarding is enabled for this zone. The value of this field contains the set of destinations to forward to. Structure is documented below.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **private\_visibility\_config** block supports:

- **networks** - (Optional) The list of VPC networks that can see this zone. Until the provider updates to use the Terraform 0.12 SDK in a future release, you may experience issues with this resource while updating. If you've defined a **networks** block and add another **networks** block while keeping the old block, Terraform will see an incorrect diff and apply an incorrect update to the resource. If you encounter this issue, remove all **networks** blocks in an update and then apply another update adding all of them back simultaneously. Structure is documented below.

The **networks** block supports:

- **network\_url** - (Optional) The fully qualified URL of the VPC network to bind to. This should be formatted like <https://www.googleapis.com/compute/v1/projects/{project}>.

The **forwarding\_config** block supports:

- **target\_name\_servers** - (Optional) List of target name servers to forward to. Cloud DNS will select the best available name server if more than one target is given. Structure is documented below.

The **target\_name\_servers** block supports:

- **ipv4\_address** - (Optional) IPv4 address of a target name server.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **name\_servers** - Delegate your managed\_zone to these virtual name servers; defined by the server

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

ManagedZone can be imported using any of these accepted formats:

```
$ terraform import google_dns_managed_zone.default projects/{{project}}/managedZones/{{name}}
$ terraform import google_dns_managed_zone.default {{project}}/{{name}}
$ terraform import google_dns_managed_zone.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_dns\_record\_set

Manages a set of DNS records within Google Cloud DNS. For more information see the official documentation and API.

**Note:** The Google Cloud DNS API requires NS records be present at all times. To accommodate this, when creating NS records, the default records Google automatically creates will be silently overwritten. Also, when destroying NS records, Terraform will not actually remove NS records, but will report that it did.

## » Example Usage

» Binding a DNS name to the ephemeral IP of a new instance:

```
resource "google_dns_record_set" "frontend" {
```

```

    name = "frontend.${google_dns_managed_zone.prod.dns_name}"
    type = "A"
    ttl = 300

    managed_zone = "${google_dns_managed_zone.prod.name}"

    rrdatas = ["${google_compute_instance.frontend.network_interface.0.access_config.0.nat_ip}"]
}

resource "google_compute_instance" "frontend" {
  name          = "frontend"
  machine_type  = "g1-small"
  zone          = "us-central1-b"

  boot_disk {
    initialize_params {
      image = "debian-cloud/debian-9"
    }
  }

  network_interface {
    network      = "default"
    access_config = {}
  }
}

resource "google_dns_managed_zone" "prod" {
  name      = "prod-zone"
  dns_name = "prod.mydomain.com."
}

```

#### » Adding an A record

```

resource "google_dns_record_set" "a" {
  name = "backend.${google_dns_managed_zone.prod.dns_name}"
  managed_zone = "${google_dns_managed_zone.prod.name}"
  type = "A"
  ttl = 300

  rrdatas = ["8.8.8.8"]
}

resource "google_dns_managed_zone" "prod" {
  name      = "prod-zone"
  dns_name = "prod.mydomain.com."
}

```



```
}
```

#### » Adding an MX record

```
resource "google_dns_record_set" "mx" {  
  name = "${google_dns_managed_zone.prod.dns_name}"  
  managed_zone = "${google_dns_managed_zone.prod.name}"  
  type = "MX"  
  ttl = 3600  
  
  rrdatas = [  
    "1 aspmx.l.google.com.",  
    "5 alt1.aspmx.l.google.com.",  
    "5 alt2.aspmx.l.google.com.",  
    "10 alt3.aspmx.l.google.com.",  
    "10 alt4.aspmx.l.google.com."  
  ]  
}
```

```
resource "google_dns_managed_zone" "prod" {  
  name = "prod-zone"  
  dns_name = "prod.mydomain.com."  
}
```

#### » Adding an SPF record

Quotes (") must be added around your rrdatas for a SPF record. Otherwise rrdatas string gets split on spaces.

```
resource "google_dns_record_set" "spf" {  
  name = "frontend.${google_dns_managed_zone.prod.dns_name}"  
  managed_zone = "${google_dns_managed_zone.prod.name}"  
  type = "TXT"  
  ttl = 300  
  
  rrdatas = ["\"v=spf1 ip4:111.111.111.111 include:backoff.email-example.com -all\""]  
}  
  
resource "google_dns_managed_zone" "prod" {  
  name = "prod-zone"  
  dns_name = "prod.mydomain.com."  
}
```

## » Adding a CNAME record

The list of `rrdatas` should only contain a single string corresponding to the Canonical Name intended.

```
resource "google_dns_record_set" "cname" {
  name = "frontend.${google_dns_managed_zone.prod.dns_name}"
  managed_zone = "${google_dns_managed_zone.prod.name}"
  type = "CNAME"
  ttl = 300
  rrdatas = ["frontend.mydomain.com."]
}

resource "google_dns_managed_zone" "prod" {
  name = "prod-zone"
  dns_name = "prod.mydomain.com."
}
```

## » Argument Reference

The following arguments are supported:

- `managed_zone` - (Required) The name of the zone in which this record set will reside.
  - `name` - (Required) The DNS name this record set will apply to.
  - `rrdatas` - (Required) The string data for the records in this record set whose meaning depends on the DNS type. For TXT record, if the string data contains spaces, add surrounding `\` if you don't want your string to get split on spaces. To specify a single record value longer than 255 characters such as a TXT record for DKIM, add `\"` inside the Terraform configuration string (e.g. `"first255characters\""`morecharacters").
  - `ttl` - (Required) The time-to-live of this record set (seconds).
  - `type` - (Required) The DNS record set type.
- 
- `project` - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » Import

DNS record set can be imported using the `zone name`, `record name` and `record type`, e.g.

```
$ terraform import google_dns_record_set.frontend prod-zone/frontend.prod.mydomain.com./A
```

Note: The record name must include the trailing dot at the end.

## » google\_\_endpoints\_\_service

This resource creates and rolls out a Cloud Endpoints service using OpenAPI or gRPC. View the relevant docs for OpenAPI and gRPC.

## » Example Usage

```
resource "google_endpoints_service" "openapi_service" {
  service_name = "api-name.endpoints.project-id.cloud.goog"
  project      = "project-id"
  openapi_config = "${file("openapi_spec.yml")}"
}

resource "google_endpoints_service" "grpc_service" {
  service_name      = "api-name.endpoints.project-id.cloud.goog"
  project           = "project-id"
  grpc_config       = "${file("service_spec.yml")}"
  protoc_output_base64 = "${base64encode(file("compiled_descriptor_file.pb"))}"
}
```

The example in `examples/endpoints_on_compute_engine` shows the API from the quickstart running on a Compute Engine VM and reachable through Cloud Endpoints, which may also be useful.

## » Argument Reference

The following arguments are supported:

- `service_name`: (Required) The name of the service. Usually of the form `$apiname.endpoints.$projectid.cloud.goog`.
- `openapi_config`: (Optional) The full text of the OpenAPI YAML configuration as described here. Either this, or *both* of `grpc_config` and `protoc_output_base64` must be specified.

- **grpc\_config:** (Optional) The full text of the Service Config YAML file (Example located here). If provided, must also provide **protoc\_output\_base64**. **open\_api** config must *not* be provided.
- **protoc\_output\_base64:** (Optional) The full contents of the Service Descriptor File generated by protoc. This should be a compiled .pb file, base64-encoded.
- **project:** (Optional) The project ID that the service belongs to. If not provided, provider project is used.

## » Attributes Reference

In addition to the arguments, the following attributes are available:

- **config\_id:** The autogenerated ID for the configuration that is rolled out as part of the creation of this resource. Must be provided to compute engine instances as a tag.
- **dns\_address:** The address at which the service can be found - usually the same as the service name.
- **apis:** A list of API objects; structure is documented below.
- **endpoints:** A list of Endpoint objects; structure is documented below.

---

## » API Object Structure

- **name:** The FQDN of the API as described in the provided config.
- **syntax:** SYNTAX\_PROTO2 or SYNTAX\_PROTO3.
- **version:** A version string for this api. If specified, will have the form major-version.minor-version, e.g. 1.10.
- **methods:** A list of Method objects; structure is documented below.

## » Method Object Structure

- **name:** The simple name of this method as described in the provided config.
- **syntax:** SYNTAX\_PROTO2 or SYNTAX\_PROTO3.
- **request\_type:** The type URL for the request to this API.
- **response\_type:** The type URL for the response from this API.

## » Endpoint Object Structure

- **name:** The simple name of the endpoint as described in the config.

- **address:** The FQDN of the endpoint as described in the config.

## » google\_filestore\_instance

A Google Cloud Filestore instance.

**Warning:** This resource is in beta, and should be used with the terraform-provider-google-beta provider. See Provider Versions for more details on beta resources.

To get more information about Instance, see:

- API documentation
- How-to Guides
  - Official Documentation
  - Use with Kubernetes
  - Copying Data In/Out



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Filestore Instance Basic

```
resource "google_filestore_instance" "instance" {
  provider = "google-beta"

  name = "test-instance"
  zone = "us-central1-b"
  tier = "PREMIUM"

  file_shares {
    capacity_gb = 2660
    name        = "share1"
  }

  networks {
    network = "default"
    modes   = ["MODE_IPV4"]
  }
}

provider "google-beta"{
```

```

    region = "us-central1"
    zone   = "us-central1-a"
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The resource name of the instance.
- **tier** - (Required) The service tier of the instance.
- **file\_shares** - (Required) File system shares on the instance. For this version, only a single file share is supported. Structure is documented below.
- **networks** - (Required) VPC networks to which the instance is connected. For this version, only a single network is supported. Structure is documented below.
- **zone** - (Required) The name of the Filestore zone of the instance.

The **file\_shares** block supports:

- **name** - (Required) The name of the fileshare (16 characters or less)
- **capacity\_gb** - (Required) File share capacity in GB.

The **networks** block supports:

- **network** - (Required) The name of the GCE VPC network to which the instance is connected.
- **modes** - (Required) IP versions for which the instance has IP addresses assigned.
- **reserved\_ip\_range** - (Optional) A /29 CIDR block that identifies the range of IP addresses reserved for this instance.
- **ip\_addresses** - A list of IPv4 or IPv6 addresses.

- 
- **description** - (Optional) A description of the instance.
  - **labels** - (Optional) Resource labels to represent user-provided metadata.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `create_time` - Creation timestamp in RFC3339 text format.
- `etag` - Server-specified ETag for the instance resource to prevent simultaneous updates from overwriting each other.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 6 minutes.
- `update` - Default is 6 minutes.
- `delete` - Default is 6 minutes.

## » Import

Instance can be imported using any of these accepted formats:

```
$ terraform import -provider=google-beta google_filestore_instance.default projects/{{project}}/zones/{{zone}}/instances/{{name}}
$ terraform import -provider=google-beta google_filestore_instance.default {{project}}/{{zone}}/{{name}}
$ terraform import -provider=google-beta google_filestore_instance.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_pubsub\_subscription

A named resource representing the stream of messages from a single, specific topic, to be delivered to the subscribing application.

To get more information about Subscription, see:

- API documentation
- How-to Guides
  - Managing Subscriptions

## » Example Usage - Pubsub Subscription Push

```
resource "google_pubsub_topic" "example" {
  name = "example-topic"
```

```

}

resource "google_pubsub_subscription" "example" {
  name = "example-subscription"
  topic = "${google_pubsub_topic.example.name}"

  ack_deadline_seconds = 20

  labels = {
    foo = "bar"
  }

  push_config {
    push_endpoint = "https://example.com/push"

    attributes {
      x-goog-version = "v1"
    }
  }
}

```



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Pubsub Subscription Pull

```

resource "google_pubsub_topic" "example" {
  name = "example-topic"
}

resource "google_pubsub_subscription" "example" {
  name = "example-subscription"
  topic = "${google_pubsub_topic.example.name}"

  labels = {
    foo = "bar"
  }

  # 20 minutes
  message_retention_duration = "1200s"
  retain_acked_messages = true

  ack_deadline_seconds = 20
}

```



}

## » Example Usage - Pubsub Subscription Different Project

```
resource "google_pubsub_topic" "example" {
  project = "topic-project"
  name    = "example-topic"
}

resource "google_pubsub_subscription" "example" {
  project = "subscription-project"
  name    = "example-subscription"
  topic   = "${google_pubsub_topic.example.id}"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Name of the subscription.
  - **topic** - (Required) A reference to a Topic resource.
- 
- **labels** - (Optional) A set of key/value label pairs to assign to this Subscription.
  - **push\_config** - (Optional) If push delivery is used with this subscription, this field is used to configure it. An empty pushConfig signifies that the subscriber will pull and ack messages using API methods. Structure is documented below.
  - **ack\_deadline\_seconds** - (Optional) This value is the maximum time after a subscriber receives a message before the subscriber should acknowledge the message. After message delivery but before the ack deadline expires and before the message is acknowledged, it is an outstanding message and will not be delivered again during that time (on a best-effort basis). For pull subscriptions, this value is used as the initial value for the ack deadline. To override this value for a given message, call `subscriptions.modifyAckDeadline` with the corresponding `ackId` if using pull. The minimum custom deadline you can specify is 10 seconds. The maximum custom deadline you can specify is 600 seconds (10 minutes). If this parameter is 0, a default value of 10 seconds is used. For push delivery, this value is also used to set the request timeout for the call to the push endpoint. If the subscriber never acknowledges the message, the Pub/Sub system will eventually redeliver the message.

- **message\_retention\_duration** - (Optional) How long to retain unacknowledged messages in the subscription's backlog, from the moment a message is published. If `retainAckedMessages` is `true`, then this also configures the retention of acknowledged messages, and thus configures how far back in time a `subscriptions.seek` can be done. Defaults to 7 days. Cannot be more than 7 days ("604800s") or less than 10 minutes ("600s"). A duration in seconds with up to nine fractional digits, terminated by 's'. Example: "600.5s".
- **retain\_acked\_messages** - (Optional) Indicates whether to retain acknowledged messages. If `true`, then messages are not expunged from the subscription's backlog, even if they are acknowledged, until they fall out of the `messageRetentionDuration` window.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The `push_config` block supports:

- **push\_endpoint** - (Required) A URL locating the endpoint to which messages should be pushed. For example, a Webhook endpoint might use "https://example.com/push".
- **attributes** - (Optional) Endpoint configuration attributes. Every endpoint has a set of API supported attributes that can be used to control different aspects of the message delivery. The currently supported attribute is `x-goog-version`, which you can use to change the format of the pushed message. This attribute indicates the version of the data expected by the endpoint. This controls the shape of the pushed message (i.e., its fields and metadata). The endpoint version is based on the version of the Pub/Sub API. If not present during the `subscriptions.create` call, it will default to the version of the API used to make such call. If not present during a `subscriptions.modifyPushConfig` call, its value will not be changed. `subscriptions.get` calls will always return a valid version, even if the subscription was created without this attribute. The possible values for this attribute are:
  - `v1beta1`: uses the push format defined in the `v1beta1` Pub/Sub API.
  - `v1` or `v1beta2`: uses the push format defined in the `v1` Pub/Sub API.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **path**: Path of the subscription in the format `projects/{project}/subscriptions/{name}`

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Subscription can be imported using any of these accepted formats:

```
$ terraform import google_pubsub_subscription.default projects/{{project}}/subscriptions/{{name}}
$ terraform import google_pubsub_subscription.default {{project}}/{{name}}
$ terraform import google_pubsub_subscription.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » IAM policy for Pubsub Subscription

Three different resources help you manage your IAM policy for pubsub subscription. Each of these resources serves a different use case:

- `google_pubsub_subscription_iam_policy`: Authoritative. Sets the IAM policy for the subscription and replaces any existing policy already attached.
- `google_pubsub_subscription_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the subscription are preserved.
- `google_pubsub_subscription_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the subscription are preserved.

**Note:** `google_pubsub_subscription_iam_policy` **cannot** be used in conjunction with `google_pubsub_subscription_iam_binding` and `google_pubsub_subscription_iam_member` or they will fight over what your policy should be.

**Note:** `google_pubsub_subscription_iam_binding` resources **can be** used in conjunction with `google_pubsub_subscription_iam_member` resources **only if** they do not grant privilege to the same role.

## » google\_pubsub\_subscription\_iam\_policy

```
data "google_iam_policy" "admin" {
  binding {
    role    = "roles/editor"
    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_pubsub_subscription_iam_policy" "editor" {
  subscription = "your-subscription-name"
  policy_data  = "${data.google_iam_policy.admin.policy_data}"
}
```

## » google\_pubsub\_subscription\_iam\_binding

```
resource "google_pubsub_subscription_iam_binding" "editor" {
  subscription = "your-subscription-name"
  role         = "roles/editor"
  members      = [
    "user:jane@example.com",
  ]
}
```

## » google\_pubsub\_subscription\_iam\_member

```
resource "google_pubsub_subscription_iam_member" "editor" {
  subscription = "your-subscription-name"
  role         = "roles/editor"
  member       = "user:jane@example.com"
}
```

## » Argument Reference

The following arguments are supported:

- **subscription** - (Required) The subscription name or id to bind to attach IAM policy to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:

- **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, alice@gmail.com or joe@example.com.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_pubsub_subscription_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
  - **policy\_data** - (Required only by `google_pubsub_subscription_iam_policy`) The policy data generated by a `google_iam_policy` data source.

- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the subscription's IAM policy.

## » Import

Pubsub subscription IAM resources can be imported using the project, subscription name, role and member.

```
$ terraform import google_pubsub_subscription_iam_policy.editor projects/{your-project-id}/subscriptions/{your-subscription-name}/policies/{your-policy-name}
$ terraform import google_pubsub_subscription_iam_binding.editor "projects/{your-project-id}/subscriptions/{your-subscription-name}/bindings/{your-binding-name}"
$ terraform import google_pubsub_subscription_iam_member.editor "projects/{your-project-id}/subscriptions/{your-subscription-name}/members/{your-member-name}"
```

## » IAM policy for Pubsub Subscription

Three different resources help you manage your IAM policy for pubsub subscription. Each of these resources serves a different use case:

- `google_pubsub_subscription_iam_policy`: Authoritative. Sets the IAM policy for the subscription and replaces any existing policy already attached.
- `google_pubsub_subscription_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the subscription are preserved.
- `google_pubsub_subscription_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the subscription are preserved.

**Note:** `google_pubsub_subscription_iam_policy` **cannot** be used in conjunction with `google_pubsub_subscription_iam_binding` and `google_pubsub_subscription_iam_member` or they will fight over what your policy should be.

**Note:** `google_pubsub_subscription_iam_binding` resources **can be** used in conjunction with `google_pubsub_subscription_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_pubsub_subscription_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role    = "roles/editor"
    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_pubsub_subscription_iam_policy" "editor" {
  subscription = "your-subscription-name"
  policy_data  = "${data.google_iam_policy.admin.policy_data}"
}
```

### » `google_pubsub_subscription_iam_binding`

```
resource "google_pubsub_subscription_iam_binding" "editor" {
  subscription = "your-subscription-name"
  role         = "roles/editor"
```

```

members      = [
  "user:jane@example.com",
]
}

```

## » google\_pubsub\_subscription\_iam\_member

```

resource "google_pubsub_subscription_iam_member" "editor" {
  subscription = "your-subscription-name"
  role         = "roles/editor"
  member       = "user:jane@example.com"
}

```

## » Argument Reference

The following arguments are supported:

- **subscription** - (Required) The subscription name or id to bind to attach IAM policy to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_pubsub_subscription_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_pubsub_subscription_iam_policy`) The policy data generated by a `google_iam_policy` data source.

- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the subscription's IAM policy.

## » Import

Pubsub subscription IAM resources can be imported using the project, subscription name, role and member.

```
$ terraform import google_pubsub_subscription_iam_policy.editor projects/{your-project-id}/s
```

```
$ terraform import google_pubsub_subscription_iam_binding.editor "projects/{your-project-id}/s
```

```
$ terraform import google_pubsub_subscription_iam_member.editor "projects/{your-project-id}/s
```

## » IAM policy for Pubsub Subscription

Three different resources help you manage your IAM policy for pubsub subscription. Each of these resources serves a different use case:

- **google\_pubsub\_subscription\_iam\_policy**: Authoritative. Sets the IAM policy for the subscription and replaces any existing policy already attached.
- **google\_pubsub\_subscription\_iam\_binding**: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the subscription are preserved.
- **google\_pubsub\_subscription\_iam\_member**: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the subscription are preserved.

**Note:** `google_pubsub_subscription_iam_policy` **cannot** be used in conjunction with `google_pubsub_subscription_iam_binding` and `google_pubsub_subscription_iam_member` or they will fight over what your policy should be.

**Note:** `google_pubsub_subscription_iam_binding` resources **can be** used in conjunction with `google_pubsub_subscription_iam_member` resources **only if** they do not grant privilege to the same role.



## » google\_pubsub\_subscription\_iam\_policy

```
data "google_iam_policy" "admin" {
  binding {
    role    = "roles/editor"
    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_pubsub_subscription_iam_policy" "editor" {
  subscription = "your-subscription-name"
  policy_data  = "${data.google_iam_policy.admin.policy_data}"
}
```

## » google\_pubsub\_subscription\_iam\_binding

```
resource "google_pubsub_subscription_iam_binding" "editor" {
  subscription = "your-subscription-name"
  role         = "roles/editor"
  members      = [
    "user:jane@example.com",
  ]
}
```

## » google\_pubsub\_subscription\_iam\_member

```
resource "google_pubsub_subscription_iam_member" "editor" {
  subscription = "your-subscription-name"
  role         = "roles/editor"
  member       = "user:jane@example.com"
}
```

## » Argument Reference

The following arguments are supported:

- **subscription** - (Required) The subscription name or id to bind to attach IAM policy to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:

- **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, alice@gmail.com or joe@example.com.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_pubsub_subscription_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
  - **policy\_data** - (Required only by `google_pubsub_subscription_iam_policy`) The policy data generated by a `google_iam_policy` data source.

- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the subscription's IAM policy.

## » Import

Pubsub subscription IAM resources can be imported using the project, subscription name, role and member.

```
$ terraform import google_pubsub_subscription_iam_policy.editor projects/{your-project-id}/subscriptions/{your-subscription-name}/policies/{your-policy-name}
$ terraform import google_pubsub_subscription_iam_binding.editor "projects/{your-project-id}/subscriptions/{your-subscription-name}/bindings/{your-binding-name}"
$ terraform import google_pubsub_subscription_iam_member.editor "projects/{your-project-id}/subscriptions/{your-subscription-name}/members/{your-member-name}"
```

## » `google__pubsub__topic`

A named resource to which messages are sent by publishers.

To get more information about Topic, see:

- API documentation
- How-to Guides
  - Managing Topics



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Pubsub Topic Basic

```
resource "google_pubsub_topic" "example" {
  name = "example-topic"

  labels = {
    foo = "bar"
  }
}
```

## » Argument Reference

The following arguments are supported:

- `name` - (Required) Name of the topic.
- 
- `labels` - (Optional) A set of key/value label pairs to assign to this Topic.
  - `project` - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Topic can be imported using any of these accepted formats:

```
$ terraform import google_pubsub_topic.default projects/{{project}}/topics/{{name}}
$ terraform import google_pubsub_topic.default {{project}}/{{name}}
$ terraform import google_pubsub_topic.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » IAM policy for Pubsub Topic

Three different resources help you manage your IAM policy for pubsub topic. Each of these resources serves a different use case:

- `google_pubsub_topic_iam_policy`: Authoritative. Sets the IAM policy for the topic and replaces any existing policy already attached.
- `google_pubsub_topic_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the topic are preserved.
- `google_pubsub_topic_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the topic are preserved.

**Note:** `google_pubsub_topic_iam_policy` **cannot** be used in conjunction with `google_pubsub_topic_iam_binding` and `google_pubsub_topic_iam_member` or they will fight over what your policy should be.

**Note:** `google_pubsub_topic_iam_binding` resources **can be** used in conjunction with `google_pubsub_topic_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_pubsub_topic_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role    = "roles/editor"
    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_pubsub_topic_iam_policy" "editor" {
```

```

    topic      = "your-topic-name"
    policy_data = "${data.google_iam_policy.admin.policy_data}"
}

```

## » google\_pubsub\_topic\_iam\_binding

```

resource "google_pubsub_topic_iam_binding" "editor" {
  topic  = "your-topic-name"
  role   = "roles/editor"
  members = [
    "user:jane@example.com",
  ]
}

```

## » google\_pubsub\_topic\_iam\_member

```

resource "google_pubsub_topic_iam_member" "editor" {
  topic  = "your-topic-name"
  role   = "roles/editor"
  member = "user:jane@example.com"
}

```

## » Argument Reference

The following arguments are supported:

- **topic** - (Required) The topic name or id to bind to attach IAM policy to.
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, alice@gmail.com or joe@example.com.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.

- **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_pubsub_topic_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_pubsub_topic_iam_policy`) The policy data generated by a `google_iam_policy` data source.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the topic's IAM policy.

## » Import

Pubsub topic IAM resources can be imported using the project, topic name, role and member.

```
$ terraform import google_pubsub_topic_iam_policy.editor projects/{your-project-id}/topics/{topic-name}
```

```
$ terraform import google_pubsub_topic_iam_binding.editor "projects/{your-project-id}/topics/{topic-name}:{role-name}:{member-name}"
```

```
$ terraform import google_pubsub_topic_iam_member.editor "projects/{your-project-id}/topics/{topic-name}:{role-name}:{member-name}"
```

## » IAM policy for Pubsub Topic

Three different resources help you manage your IAM policy for pubsub topic. Each of these resources serves a different use case:

- **google\_pubsub\_topic\_iam\_policy**: Authoritative. Sets the IAM policy for the topic and replaces any existing policy already attached.
- **google\_pubsub\_topic\_iam\_binding**: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the topic are preserved.
- **google\_pubsub\_topic\_iam\_member**: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the topic are preserved.

**Note:** `google_pubsub_topic_iam_policy` **cannot** be used in conjunction with `google_pubsub_topic_iam_binding` and `google_pubsub_topic_iam_member` or they will fight over what your policy should be.

**Note:** `google_pubsub_topic_iam_binding` resources **can be** used in conjunction with `google_pubsub_topic_iam_member` resources **only if** they do not grant privilege to the same role.

## » `google_pubsub_topic_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role    = "roles/editor"
    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_pubsub_topic_iam_policy" "editor" {
  topic      = "your-topic-name"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

## » `google_pubsub_topic_iam_binding`

```
resource "google_pubsub_topic_iam_binding" "editor" {
  topic    = "your-topic-name"
  role     = "roles/editor"
  members = [
    "user:jane@example.com",
  ]
}
```

## » `google_pubsub_topic_iam_member`

```
resource "google_pubsub_topic_iam_member" "editor" {
  topic    = "your-topic-name"
  role     = "roles/editor"
  member   = "user:jane@example.com"
}
```

## » Argument Reference

The following arguments are supported:

- **topic** - (Required) The topic name or id to bind to attach IAM policy to.
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_pubsub_topic_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_pubsub_topic_iam_policy`) The policy data generated by a `google_iam_policy` data source.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the topic's IAM policy.

## » Import

Pubsub topic IAM resources can be imported using the project, topic name, role and member.

```
$ terraform import google_pubsub_topic_iam_policy.editor projects/{your-project-id}/topics/{topic-name}/roles/{role-name}
```



```
$ terraform import google_pubsub_topic_iam_binding.editor "projects/{your-project-id}/topics/
$ terraform import google_pubsub_topic_iam_member.editor "projects/{your-project-id}/topics/
```

## » IAM policy for Pubsub Topic

Three different resources help you manage your IAM policy for pubsub topic. Each of these resources serves a different use case:

- `google_pubsub_topic_iam_policy`: Authoritative. Sets the IAM policy for the topic and replaces any existing policy already attached.
- `google_pubsub_topic_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the topic are preserved.
- `google_pubsub_topic_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the topic are preserved.

**Note:** `google_pubsub_topic_iam_policy` **cannot** be used in conjunction with `google_pubsub_topic_iam_binding` and `google_pubsub_topic_iam_member` or they will fight over what your policy should be.

**Note:** `google_pubsub_topic_iam_binding` resources **can be** used in conjunction with `google_pubsub_topic_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_pubsub_topic_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role    = "roles/editor"
    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_pubsub_topic_iam_policy" "editor" {
  topic      = "your-topic-name"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

## » google\_pubsub\_topic\_iam\_binding

```
resource "google_pubsub_topic_iam_binding" "editor" {
  topic    = "your-topic-name"
  role     = "roles/editor"
  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_pubsub\_topic\_iam\_member

```
resource "google_pubsub_topic_iam_member" "editor" {
  topic    = "your-topic-name"
  role     = "roles/editor"
  member   = "user:jane@example.com"
}
```

## » Argument Reference

The following arguments are supported:

- **topic** - (Required) The topic name or id to bind to attach IAM policy to.
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.

- **role** - (Required) The role that should be applied. Only one `google_pubsub_topic_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_pubsub_topic_iam_policy`) The policy data generated by a `google_iam_policy` data source.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the topic's IAM policy.

## » Import

Pubsub topic IAM resources can be imported using the project, topic name, role and member.

```
$ terraform import google_pubsub_topic_iam_policy.editor projects/{your-project-id}/topics/{topic-name}
```

```
$ terraform import google_pubsub_topic_iam_binding.editor "projects/{your-project-id}/topics/{topic-name}:{role-name}:{member-name}"
```

```
$ terraform import google_pubsub_topic_iam_member.editor "projects/{your-project-id}/topics/{topic-name}:{role-name}:{member-name}"
```

## » google\_\_redis\_\_instance

A Google Cloud Redis instance.

To get more information about Instance, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Redis Instance Basic

```
resource "google_redis_instance" "cache" {
  name = "memory-cache"
```

```
memory_size_gb = 1
}
```



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Redis Instance Full

```
resource "google_redis_instance" "cache" {
  name          = "ha-memory-cache"
  tier           = "STANDARD_HA"
  memory_size_gb = 1

  location_id          = "us-central1-a"
  alternative_location_id = "us-central1-f"

  authorized_network = "${google_compute_network.auto-network.self_link}"

  redis_version      = "REDIS_3_2"
  display_name       = "Terraform Test Instance"
  reserved_ip_range = "192.168.0.0/29"

  labels = {
    my_key    = "my_val"
    other_key = "other_val"
  }
}

resource "google_compute_network" "auto-network" {
  name = "authorized-network"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The ID of the instance or a fully qualified identifier for the instance.
- **memory\_size\_gb** - (Required) Redis memory size in GiB.

- **alternative\_location\_id** - (Optional) Only applicable to STANDARD\_HA tier which protects the instance against zonal failures by provisioning it across two zones. If provided, it must be a different zone from the one provided in [locationId].
- **authorized\_network** - (Optional) The full name of the Google Compute Engine network to which the instance is connected. If left unspecified, the default network will be used.
- **display\_name** - (Optional) An arbitrary and optional user-provided name for the instance.
- **labels** - (Optional) Resource labels to represent user provided metadata.
- **redis\_configs** - (Optional) Redis configuration parameters, according to <http://redis.io/topics/config>. Please check Memorystore documentation for the list of supported parameters: [https://cloud.google.com/memorystore/docs/redis/reference/rest/v1/projects.locations.instances#Instance.FIELDS.redis\\_configs](https://cloud.google.com/memorystore/docs/redis/reference/rest/v1/projects.locations.instances#Instance.FIELDS.redis_configs)
- **location\_id** - (Optional) The zone where the instance will be provisioned. If not provided, the service will choose a zone for the instance. For STANDARD\_HA tier, instances will be created across two zones for protection against zonal failures. If [alternativeLocationId] is also provided, it must be different from [locationId].
- **redis\_version** - (Optional) The version of Redis software. If not provided, latest supported version will be used. Updating the version will perform an upgrade/downgrade to the new version. Currently, the supported values are REDIS\_3\_2 for Redis 3.2.
- **reserved\_ip\_range** - (Optional) The CIDR range of internal addresses that are reserved for this instance. If not provided, the service will choose an unused /29 block, for example, 10.0.0.0/29 or 192.168.0.0/29. Ranges must be unique and non-overlapping with existing subnets in an authorized network.
- **tier** - (Optional) The service tier of the instance. Must be one of these values:
  - BASIC: standalone instance
  - STANDARD\_HA: highly available primary/replica instances
- **region** - (Optional) The name of the Redis region of the instance.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **create\_time** - The time the instance was created in RFC3339 UTC "Zulu" format, accurate to nanoseconds.
- **current\_location\_id** - The current zone where the Redis endpoint is placed. For Basic Tier instances, this will always be the same as the [locationId] provided by the user at creation time. For Standard Tier instances, this can be either [locationId] or [alternativeLocationId] and can change after a failover event.
- **host** - Hostname or IP address of the exposed Redis endpoint used by clients to connect to the service.
- **port** - The port number of the exposed Redis endpoint.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 6 minutes.
- **update** - Default is 6 minutes.
- **delete** - Default is 6 minutes.

## » Import

Instance can be imported using any of these accepted formats:

```
$ terraform import google_redis_instance.default projects/{{project}}/locations/{{region}}/instances/{{name}}
$ terraform import google_redis_instance.default {{project}}/{{region}}/{{name}}
$ terraform import google_redis_instance.default {{name}}
```

If you're importing a resource with beta features, make sure to include **-provider=google-beta** as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_runtimeconfig\_\_config

Manages a RuntimeConfig resource in Google Cloud. For more information, see the official documentation, or the JSON API.

## » Example Usage

Example creating a RuntimeConfig resource.

```
resource "google_runtimeconfig_config" "my-runtime-config" {
  name = "my-service-runtime-config"
  description = "Runtime configuration values for my service"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the runtime config.
- 
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
  - **description** - (Optional) The description to associate with the runtime config.

## » Import

Runtime Configs can be imported using the **name** or full config name, e.g.

```
$ terraform import google_runtimeconfig_config.myconfig myconfig
```

```
$ terraform import google_runtimeconfig_config.myconfig projects/my-gcp-project/configs/myconfig
```

When importing using only the name, the provider project must be set.

## » google\_\_runtimeconfig\_\_variable

Manages a RuntimeConfig variable in Google Cloud. For more information, see the official documentation, or the JSON API.

## » Example Usage

Example creating a RuntimeConfig variable.

```
resource "google_runtimeconfig_config" "my-runtime-config" {
  name = "my-service-runtime-config"
  description = "Runtime configuration values for my service"
}
```

```
resource "google_runtimeconfig_variable" "environment" {
  parent = "${google_runtimeconfig_config.my-runtime-config.name}"
  name = "prod-variables/hostname"
  text = "example.com"
}
```

You can also encode binary content using the `value` argument instead. The value must be base64 encoded.

Example of using the `value` argument.

```
resource "google_runtimeconfig_config" "my-runtime-config" {
  name = "my-service-runtime-config"
  description = "Runtime configuration values for my service"
}

resource "google_runtimeconfig_variable" "my-secret" {
  parent = "${google_runtimeconfig_config.my-runtime-config.name}"
  name = "secret"
  value = "${base64encode(file("my-encrypted-secret.dat"))}"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the variable to manage. Note that variable names can be hierarchical using slashes (e.g. "prod-variables/hostname").
  - **parent** - (Required) The name of the RuntimeConfig resource containing this variable.
  - **text** or **value** - (Required) The content to associate with the variable. Exactly one of `text` or `value` must be specified. If `text` is specified, it must be a valid UTF-8 string and less than 4096 bytes in length. If `value` is specified, it must be base64 encoded and less than 4096 bytes in length.
- 
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:



- `update_time` - (Computed) The timestamp in RFC3339 UTC "Zulu" format, accurate to nanoseconds, representing when the variable was last updated. Example: "2016-10-09T12:33:37.578138407Z".

## » Import

Runtime Config Variables can be imported using the `name` or full variable name, e.g.

```
$ terraform import google_runtimeconfig_variable.myvariable myconfig/myvariable
$ terraform import google_runtimeconfig_variable.myvariable projects/my-gcp-project/configs/
```

When importing using only the name, the provider project must be set.

## » `google_service_networking_connection`

**Warning:** This resource is in beta, and should be used with the terraform-provider-google-beta provider. See Provider Versions for more details on beta resources.

Manages a private VPC connection with a GCP service provider. For more information see the official documentation and API.

## » Example usage

```
resource "google_compute_network" "peering_network" {
  name = "peering_network"
}

resource "google_compute_global_address" "private_ip_alloc" {
  name          = "private_ip_alloc"
  purpose       = "VPC_PEERING"
  address_type  = "INTERNAL"
  prefix_length = 16
  network       = "${google_compute_network.peering_network.self_link}"
}

resource "google_service_networking_connection" "foobar" {
  network          = "${google_compute_network.peering_network.self_link}"
  service          = "servicenetworking.googleapis.com"
  reserved_peering_ranges = ["${google_compute_global_address.private_ip_alloc.name}"]
}
```

## » Argument Reference

The following arguments are supported:

- **network** - (Required) Name of VPC network connected with service producers using VPC peering.
- **service** - (Required) Provider peering service that is managing peering connectivity for a service provider organization. For Google services that support this functionality it is 'servicenetworking.googleapis.com'.
- **reserved\_peering\_ranges** - (Required) Named IP address range(s) of PEERING type reserved for this service provider. Note that invoking this method with a different range when connection is already established will not reallocate already provisioned service producer subnetworks.

## » google\_\_sourcerepo\_\_repository

A repository (or repo) is a Git repository storing versioned source content.

To get more information about Repository, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Sourcerepo Repository Basic

```
resource "google_sourcerepo_repository" "my-repo" {  
  name = "my-repository"  
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) Resource name of the repository, of the form {{repo}}. The repo name may contain slashes. eg, **name/with/slash**

- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **url** - URL to clone the repository from Google Cloud Source Repositories.
- **size** - The disk usage of the repo, in bytes.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

Repository can be imported using any of these accepted formats:

```
$ terraform import google_sourcerepo_repository.default projects/{{project}}/repos/{{name}}
$ terraform import google_sourcerepo_repository.default {{project}}/{{name}}
$ terraform import google_sourcerepo_repository.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_spanner\_\_database

A Cloud Spanner Database which is hosted on a Spanner instance.

To get more information about Database, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Spanner Database Basic

```
resource "google_spanner_instance" "main" {
  config      = "regional-europe-west1"
  display_name = "main-instance"
}

resource "google_spanner_database" "database" {
  instance = "${google_spanner_instance.main.name}"
  name     = "my-database"
  ddl      = [
    "CREATE TABLE t1 (t1 INT64 NOT NULL,) PRIMARY KEY(t1)",
    "CREATE TABLE t2 (t2 INT64 NOT NULL,) PRIMARY KEY(t2)"
  ]
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique identifier for the database, which cannot be changed after the instance is created. Values are of the form [a-z][a-z0-9]\*[a-z0-9].
  - **instance** - (Required) The instance to create the database on.
- 
- **ddl** - (Optional) An optional list of DDL statements to run inside the newly created database. Statements can create tables, indexes, etc. These statements execute atomically with the creation of the database: if there is an error in any statement, the database is not created.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **state** - An explanation of the status of the database.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

Database can be imported using any of these accepted formats:

```
$ terraform import google_spanner_database.default projects/{{project}}/instances/{{instance}}
$ terraform import google_spanner_database.default instances/{{instance}}/databases/{{name}}
$ terraform import google_spanner_database.default {{project}}/{{instance}}/{{name}}
$ terraform import google_spanner_database.default {{instance}}/{{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » IAM policy for Spanner databases

Three different resources help you manage your IAM policy for a Spanner database. Each of these resources serves a different use case:

- `google_spanner_database_iam_policy`: Authoritative. Sets the IAM policy for the database and replaces any existing policy already attached.

**Warning:** It's entirely possible to lock yourself out of your database using `google_spanner_database_iam_policy`. Any permissions granted by default will be removed unless you include them in your config.

- `google_spanner_database_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the database are preserved.
- `google_spanner_database_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the database are preserved.

**Note:** `google_spanner_database_iam_policy` **cannot** be used in conjunction with `google_spanner_database_iam_binding` and `google_spanner_database_iam_member` or they will fight over what your policy should be.

**Note:** `google_spanner_database_iam_binding` resources **can be** used in conjunction with `google_spanner_database_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_spanner_database_iam_policy`

```
data "google_iam_policy" "admin" {
```

```

binding {
  role = "roles/editor"

  members = [
    "user:jane@example.com",
  ]
}

resource "google_spanner_database_iam_policy" "database" {
  instance      = "your-instance-name"
  database      = "your-database-name"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}

```

#### » google\_spanner\_database\_iam\_binding

```

resource "google_spanner_database_iam_binding" "database" {
  instance      = "your-instance-name"
  database      = "your-database-name"
  role          = "roles/compute.networkUser"

  members = [
    "user:jane@example.com",
  ]
}

```

#### » google\_spanner\_database\_iam\_member

```

resource "google_spanner_database_iam_member" "database" {
  instance      = "your-instance-name"
  database      = "your-database-name"
  role          = "roles/compute.networkUser"
  member        = "user:jane@example.com"
}

```

### » Argument Reference

The following arguments are supported:

- **database** - (Required) The name of the Spanner database.
- **instance** - (Required) The name of the Spanner instance the database belongs to.

- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, alice@gmail.com or joe@example.com.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_spanner_database_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_spanner_database_iam_policy`) The policy data generated by a `google_iam_policy` data source.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the database's IAM policy.

## » Import

For all import syntaxes, the "resource in question" can take any of the following forms:

- `{{project}}/{{instance}}/{{database}}`
- `{{instance}}/{{database}}` (project is taken from provider project)

IAM member imports use space-delimited identifiers; the resource in question, the role, and the member identity, e.g.

```
$ terraform import google_spanner_database_iam_member.database "project-name/instance-name/role-name/member-name"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role, e.g.

```
$ terraform import google_spanner_database_iam_binding.database "project-name/instance-name/da
```

IAM policy imports use the identifier of the resource in question, e.g.

```
$ terraform import google_spanner_database_iam_policy.database project-name/instance-name/da
```

## » IAM policy for Spanner databases

Three different resources help you manage your IAM policy for a Spanner database. Each of these resources serves a different use case:

- `google_spanner_database_iam_policy`: Authoritative. Sets the IAM policy for the database and replaces any existing policy already attached.

**Warning:** It's entirely possible to lock yourself out of your database using `google_spanner_database_iam_policy`. Any permissions granted by default will be removed unless you include them in your config.

- `google_spanner_database_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the database are preserved.
- `google_spanner_database_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the database are preserved.

**Note:** `google_spanner_database_iam_policy` **cannot** be used in conjunction with `google_spanner_database_iam_binding` and `google_spanner_database_iam_member` or they will fight over what your policy should be.

**Note:** `google_spanner_database_iam_binding` resources **can be** used in conjunction with `google_spanner_database_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_spanner__database__iam__policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}
```



```
resource "google_spanner_database_iam_policy" "database" {
  instance      = "your-instance-name"
  database      = "your-database-name"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

## » google\_spanner\_database\_iam\_binding

```
resource "google_spanner_database_iam_binding" "database" {
  instance      = "your-instance-name"
  database      = "your-database-name"
  role          = "roles/compute.networkUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_spanner\_database\_iam\_member

```
resource "google_spanner_database_iam_member" "database" {
  instance      = "your-instance-name"
  database      = "your-database-name"
  role          = "roles/compute.networkUser"
  member        = "user:jane@example.com"
}
```

## » Argument Reference

The following arguments are supported:

- **database** - (Required) The name of the Spanner database.
- **instance** - (Required) The name of the Spanner instance the database belongs to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.

- **user:{emailid}**: An email address that represents a specific Google account. For example, alice@gmail.com or joe@example.com.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_spanner_database_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
  - **policy\_data** - (Required only by `google_spanner_database_iam_policy`) The policy data generated by a `google_iam_policy` data source.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the database's IAM policy.

## » Import

For all import syntaxes, the "resource in question" can take any of the following forms:

- `{{project}}/{{instance}}/{{database}}`
- `{{instance}}/{{database}}` (project is taken from provider project)

IAM member imports use space-delimited identifiers; the resource in question, the role, and the member identity, e.g.

```
$ terraform import google_spanner_database_iam_member.database "project-name/instance-name/role-name/member-identity"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role, e.g.

```
$ terraform import google_spanner_database_iam_binding.database "project-name/instance-name/role-name"
```

IAM policy imports use the identifier of the resource in question, e.g.

```
$ terraform import google_spanner_database_iam_policy.database project-name/instance-name/database-name
```

## » IAM policy for Spanner databases

Three different resources help you manage your IAM policy for a Spanner database. Each of these resources serves a different use case:

- `google_spanner_database_iam_policy`: Authoritative. Sets the IAM policy for the database and replaces any existing policy already attached.

**Warning:** It's entirely possible to lock yourself out of your database using `google_spanner_database_iam_policy`. Any permissions granted by default will be removed unless you include them in your config.

- `google_spanner_database_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the database are preserved.
- `google_spanner_database_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the database are preserved.

**Note:** `google_spanner_database_iam_policy` **cannot** be used in conjunction with `google_spanner_database_iam_binding` and `google_spanner_database_iam_member` or they will fight over what your policy should be.

**Note:** `google_spanner_database_iam_binding` resources **can be** used in conjunction with `google_spanner_database_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_spanner_database_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_spanner_database_iam_policy" "database" {
  instance      = "your-instance-name"
  database      = "your-database-name"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

## » google\_spanner\_database\_iam\_binding

```
resource "google_spanner_database_iam_binding" "database" {
  instance = "your-instance-name"
  database = "your-database-name"
  role     = "roles/compute.networkUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_spanner\_database\_iam\_member

```
resource "google_spanner_database_iam_member" "database" {
  instance = "your-instance-name"
  database = "your-database-name"
  role     = "roles/compute.networkUser"
  member   = "user:jane@example.com"
}
```

## » Argument Reference

The following arguments are supported:

- **database** - (Required) The name of the Spanner database.
- **instance** - (Required) The name of the Spanner instance the database belongs to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.

- **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_spanner_database_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_spanner_database_iam_policy`) The policy data generated by a `google_iam_policy` data source.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the database's IAM policy.

## » Import

For all import syntaxes, the "resource in question" can take any of the following forms:

- `{{project}}/{{instance}}/{{database}}`
- `{{instance}}/{{database}}` (project is taken from provider project)

IAM member imports use space-delimited identifiers; the resource in question, the role, and the member identity, e.g.

```
$ terraform import google_spanner_database_iam_member.database "project-name/instance-name/role-name/member-identity"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role, e.g.

```
$ terraform import google_spanner_database_iam_binding.database "project-name/instance-name/role-name"
```

IAM policy imports use the identifier of the resource in question, e.g.

```
$ terraform import google_spanner_database_iam_policy.database project-name/instance-name/database-name
```

## » google\_\_spanner\_\_instance

An isolated set of Cloud Spanner resources on which databases can be hosted.

To get more information about Instance, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Spanner Instance Basic

```
resource "google_spanner_instance" "example" {
  config      = "regional-us-central1"
  display_name = "Test Spanner Instance"
  num_nodes   = 2
  labels = {
    "foo" = "bar"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique identifier for the instance, which cannot be changed after the instance is created. The name must be between 6 and 30 characters in length.

If not provided, a random string starting with **tf-** will be selected.

- **config** - (Required) The name of the instance's configuration (similar but not quite the same as a region) which defines the geographic placement and replication of your databases in this instance. It determines where your data is stored. Values are typically of the form **regional-europe-west1**, **us-central** etc. In order to obtain a valid list please consult the Configuration section of the docs.
- **display\_name** - (Required) The descriptive name for this instance as it appears in UIs. Must be unique per project and between 4 and 30 characters in length.

- 
- **num\_nodes** - (Optional) The number of nodes allocated to this instance.
  - **labels** - (Optional) An object containing a list of "key": value pairs. Example: { "name": "wrench", "mass": "1.3kg", "count": "3" }.

- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **state** - Instance status: `CREATING` or `READY`.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

Instance can be imported using any of these accepted formats:

```
$ terraform import google_spanner_instance.default projects/{{project}}/instances/{{name}}
$ terraform import google_spanner_instance.default {{project}}/{{name}}
$ terraform import google_spanner_instance.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » IAM policy for Spanner Instances

Three different resources help you manage your IAM policy for a Spanner instance. Each of these resources serves a different use case:

- **google\_spanner\_instance\_iam\_policy**: Authoritative. Sets the IAM policy for the instance and replaces any existing policy already attached.

**Warning:** It's entirely possible to lock yourself out of your instance using **google\_spanner\_instance\_iam\_policy**. Any permissions granted by default will be removed unless you include them in your config.

- **google\_spanner\_instance\_iam\_binding**: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the instance are preserved.

- `google_spanner_instance_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the instance are preserved.

**Note:** `google_spanner_instance_iam_policy` **cannot** be used in conjunction with `google_spanner_instance_iam_binding` and `google_spanner_instance_iam_member` or they will fight over what your policy should be.

**Note:** `google_spanner_instance_iam_binding` resources **can be** used in conjunction with `google_spanner_instance_iam_member` resources **only if** they do not grant privilege to the same role.

## » `google_spanner_instance_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_spanner_instance_iam_policy" "instance" {
  instance      = "your-instance-name"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

## » `google_spanner_instance_iam_binding`

```
resource "google_spanner_instance_iam_binding" "instance" {
  instance = "your-instance-name"
  role     = "roles/compute.networkUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » `google_spanner_instance_iam_member`

```
resource "google_spanner_instance_iam_member" "instance" {
  instance = "your-instance-name"
```



```

    role      = "roles/compute.networkUser"
    member    = "user:jane@example.com"
  }

```

## » Argument Reference

The following arguments are supported:

- **instance** - (Required) The name of the instance.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_spanner_instance_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_spanner_instance_iam_policy`) The policy data generated by a `google_iam_policy` data source.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the instance's IAM policy.

## » Import

For all import syntaxes, the "resource in question" can take any of the following forms:

- `{{project}}/{{name}}`
- `{{name}}` (project is taken from provider project)

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account, e.g.

```
$ terraform import google_spanner_instance_iam_member.instance "project-name/instance-name member-role@project-name.iam.gcpusercontent.com"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role, e.g.

```
$ terraform import google_spanner_instance_iam_binding.instance "project-name/instance-name member-role@project-name.iam.gcpusercontent.com"
```

IAM policy imports use the identifier of the resource in question, e.g.

```
$ terraform import google_spanner_instance_iam_policy.instance project-name/instance-name
```

## » IAM policy for Spanner Instances

Three different resources help you manage your IAM policy for a Spanner instance. Each of these resources serves a different use case:

- `google_spanner_instance_iam_policy`: Authoritative. Sets the IAM policy for the instance and replaces any existing policy already attached.

**Warning:** It's entirely possible to lock yourself out of your instance using `google_spanner_instance_iam_policy`. Any permissions granted by default will be removed unless you include them in your config.

- `google_spanner_instance_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the instance are preserved.
- `google_spanner_instance_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the instance are preserved.

**Note:** `google_spanner_instance_iam_policy` **cannot** be used in conjunction with `google_spanner_instance_iam_binding` and `google_spanner_instance_iam_member` or they will fight over what your policy should be.

**Note:** `google_spanner_instance_iam_binding` resources **can be** used in conjunction with `google_spanner_instance_iam_member` resources **only if** they do not grant privilege to the same role.

## » google\_spanner\_instance\_iam\_policy

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_spanner_instance_iam_policy" "instance" {
  instance      = "your-instance-name"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

## » google\_spanner\_instance\_iam\_binding

```
resource "google_spanner_instance_iam_binding" "instance" {
  instance = "your-instance-name"
  role     = "roles/compute.networkUser"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_spanner\_instance\_iam\_member

```
resource "google_spanner_instance_iam_member" "instance" {
  instance = "your-instance-name"
  role     = "roles/compute.networkUser"
  member   = "user:jane@example.com"
}
```

## » Argument Reference

The following arguments are supported:

- **instance** - (Required) The name of the instance.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:

- **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, alice@gmail.com or joe@example.com.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_spanner_instance_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
  - **policy\_data** - (Required only by `google_spanner_instance_iam_policy`) The policy data generated by a `google_iam_policy` data source.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the instance's IAM policy.

## » Import

For all import syntaxes, the "resource in question" can take any of the following forms:

- `{{project}}/{{name}}`
- `{{name}}` (project is taken from provider project)

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account, e.g.

```
$ terraform import google_spanner_instance_iam_member.instance "project-name/instance-name 1
```

IAM binding imports use space-delimited identifiers; the resource in question and the role, e.g.

```
$ terraform import google_spanner_instance_iam_binding.instance "project-name/instance-name"
```

IAM policy imports use the identifier of the resource in question, e.g.

```
$ terraform import google_spanner_instance_iam_policy.instance project-name/instance-name
```

## » IAM policy for Spanner Instances

Three different resources help you manage your IAM policy for a Spanner instance. Each of these resources serves a different use case:

- `google_spanner_instance_iam_policy`: Authoritative. Sets the IAM policy for the instance and replaces any existing policy already attached.

**Warning:** It's entirely possible to lock yourself out of your instance using `google_spanner_instance_iam_policy`. Any permissions granted by default will be removed unless you include them in your config.

- `google_spanner_instance_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the instance are preserved.
- `google_spanner_instance_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the instance are preserved.

**Note:** `google_spanner_instance_iam_policy` **cannot** be used in conjunction with `google_spanner_instance_iam_binding` and `google_spanner_instance_iam_member` or they will fight over what your policy should be.

**Note:** `google_spanner_instance_iam_binding` resources **can be** used in conjunction with `google_spanner_instance_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_spanner_instance_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_spanner_instance_iam_policy" "instance" {
  instance = "your-instance-name"
```

```

    policy_data = "${data.google_iam_policy.admin.policy_data}"
}

```

## » google\_spanner\_instance\_iam\_binding

```

resource "google_spanner_instance_iam_binding" "instance" {
  instance = "your-instance-name"
  role     = "roles/compute.networkUser"

  members = [
    "user:jane@example.com",
  ]
}

```

## » google\_spanner\_instance\_iam\_member

```

resource "google_spanner_instance_iam_member" "instance" {
  instance = "your-instance-name"
  role     = "roles/compute.networkUser"
  member   = "user:jane@example.com"
}

```

## » Argument Reference

The following arguments are supported:

- **instance** - (Required) The name of the instance.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.

- **role** - (Required) The role that should be applied. Only one `google_spanner_instance_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_spanner_instance_iam_policy`) The policy data generated by a `google_iam_policy` data source.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the instance's IAM policy.

## » Import

For all import syntaxes, the "resource in question" can take any of the following forms:

- `{{project}}/{{name}}`
- `{{name}}` (project is taken from provider project)

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account, e.g.

```
$ terraform import google_spanner_instance_iam_member.instance "project-name/instance-name role account"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role, e.g.

```
$ terraform import google_spanner_instance_iam_binding.instance "project-name/instance-name role"
```

IAM policy imports use the identifier of the resource in question, e.g.

```
$ terraform import google_spanner_instance_iam_policy.instance project-name/instance-name
```

## » google\_\_sql\_\_database

Creates a new Google SQL Database on a Google SQL Database Instance. For more information, see the official documentation, or the JSON API.

## » Example Usage

Example creating a SQL Database.

```
resource "google_sql_database_instance" "master" {
  name = "master-instance"

  settings {
    tier = "D0"
  }
}

resource "google_sql_database" "users" {
  name      = "users-db"
  instance  = "${google_sql_database_instance.master.name}"
  charset   = "latin1"
  collation = "latin1_swedish_ci"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the database.
  - **instance** - (Required) The name of containing instance.
- 
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
  - **charset** - (Optional) The charset value. See MySQL's Supported Character Sets and Collations and Postgres' Character Set Support for more details and supported values. Postgres databases are in beta and have limited **charset** support; they only support a value of **UTF8** at creation time.
  - **collation** - (Optional) The collation value. See MySQL's Supported Character Sets and Collations and Postgres' Collation Support for more details and supported values. Postgres databases are in beta and have limited **collation** support; they only support a value of **en\_US.UTF8** at creation time.



## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `self_link` - The URI of the created resource.

## » Import

SQL databases can be imported using one of any of these accepted formats:

```
$ terraform import google_sql_database.database projects/{{project}}/instances/{{instance}}/  
$ terraform import google_sql_database.database {{project}}/{{instance}}/{{name}}  
$ terraform import google_sql_database.database instances/{{name}}/databases/{{name}}  
$ terraform import google_sql_database.database {{instance}}/{{name}}  
$ terraform import google_sql_database.database {{name}}
```

## » google\_sql\_database\_instance

Creates a new Google SQL Database Instance. For more information, see the official documentation, or the JSON API.

**NOTE on google\_sql\_database\_instance:** - Second-generation instances include a default 'root'@'%' user with no password. This user will be deleted by Terraform on instance creation. You should use `google_sql_user` to define a custom user with a restricted host and strong password.

## » Example Usage

### » SQL First Generation

```
resource "google_sql_database_instance" "master" {  
  name = "master-instance"  
  database_version = "MYSQL_5_6"  
  # First-generation instance regions are not the conventional  
  # Google Compute Engine regions. See argument reference below.  
  region = "us-central"  
  
  settings {  
    tier = "DO"  
  }  
}
```

## » SQL Second generation

```
resource "google_sql_database_instance" "master" {
  name = "master-instance"
  database_version = "POSTGRES_9_6"
  region = "us-central1"

  settings {
    # Second-generation instance tiers are based on the machine
    # type. See argument reference below.
    tier = "db-f1-micro"
  }
}
```

## » Granular restriction of network access

```
resource "google_compute_instance" "apps" {
  count          = 8
  name           = "apps-${count.index + 1}"
  machine_type   = "f1-micro"

  boot_disk {
    initialize_params {
      image = "ubuntu-os-cloud/ubuntu-1804-lts"
    }
  }

  network_interface {
    network = "default"

    access_config {
      // Ephemeral IP
    }
  }
}

data "null_data_source" "auth_netw_postgres_allowed_1" {
  count = "${length(google_compute_instance.apps.*.self_link)}"

  inputs = {
    name = "apps-${count.index + 1}"
    value = "${element(google_compute_instance.apps.*.network_interface.0.access_config.0.na"
  }
}
```

```

data "null_data_source" "auth_netw_postgres_allowed_2" {
  count = 2

  inputs = {
    name = "onprem-${count.index + 1}"
    value = "${element(list("192.168.1.2", "192.168.2.3"), count.index)}"
  }
}

resource "google_sql_database_instance" "postgres" {
  name = "postgres-instance"
  database_version = "POSTGRES_9_6"

  settings {
    tier = "db-f1-micro"

    ip_configuration {
      authorized_networks = [
        "${data.null_data_source.auth_netw_postgres_allowed_1.*.outputs}",
        "${data.null_data_source.auth_netw_postgres_allowed_2.*.outputs}",
      ]
    }
  }
}

```

#### » Private IP Instance

```

resource "google_compute_network" "private_network" {
  name = "private-network"
}

resource "google_compute_global_address" "private_ip_address" {
  name          = "private-ip-address"
  purpose       = "VPC_PEERING"
  address_type  = "INTERNAL"
  prefix_length = 16
  network       = "${google_compute_network.private_network.self_link}"
}

resource "google_service_networking_connection" "private_vpc_connection" {
  network       = "${google_compute_network.private_network.self_link}"
  service       = "servicenetworking.googleapis.com"
  reserved_peering_ranges = ["${google_compute_global_address.private_ip_address.name}"]
}

```

```

resource "google_sql_database_instance" "instance" {
  depends_on = ["google_service_networking_connection.private_vpc_connection"]
  name = "private-instance"
  region = "us-central1"
  settings {
    tier = "db-f1-micro"
    ip_configuration {
      ipv4_enabled = "false"
      private_network = "${google_compute_network.private_network.self_link}"
    }
  }
}

```

## » Argument Reference

The following arguments are supported:

- **region** - (Required) The region the instance will sit in. Note, first-generation Cloud SQL instance regions do not line up with the Google Compute Engine (GCE) regions, and Cloud SQL is not available in all regions - choose from one of the options listed here. A valid region must be provided to use this resource. If a region is not provided in the resource definition, the provider region will be used instead, but this will be an apply-time error for all first-generation instances *and* for second-generation instances if the provider region is not supported with Cloud SQL. If you choose not to provide the **region** argument for this resource, make sure you understand this.
  - **settings** - (Required) The settings to use for the database. The configuration is detailed below.
- 
- **database\_version** - (Optional, Default: `MYSQL_5_6`) The MySQL version to use. Can be `MYSQL_5_6`, `MYSQL_5_7` or `POSTGRES_9_6` for second-generation instances, or `MYSQL_5_5` or `MYSQL_5_6` for first-generation instances. See Second Generation Capabilities for more information.
  - **name** - (Optional, Computed) The name of the instance. If the name is left blank, Terraform will randomly generate one when the instance is first created. This is done because after a name is used, it cannot be reused for up to one week.
  - **master\_instance\_name** - (Optional) The name of the instance that will act as the master in the replication setup. Note, this requires the master to have `binary_log_enabled` set, as well as existing backups.

- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
- **replica\_configuration** - (Optional) The configuration for replication. The configuration is detailed below.

The required **settings** block supports:

- **tier** - (Required) The machine tier (First Generation) or type (Second Generation) to use. See tiers for more details and supported versions. Postgres supports only shared-core machine types such as **db-f1-micro**, and custom machine types such as **db-custom-2-13312**. See the Custom Machine Type Documentation to learn about specifying custom machine types.
- **activation\_policy** - (Optional) This specifies when the instance should be active. Can be either **ALWAYS**, **NEVER** or **ON\_DEMAND**.
- **authorized\_gae\_applications** - (Optional) A list of Google App Engine (GAE) project names that are allowed to access this instance.
- **availability\_type** - (Optional) This specifies whether a PostgreSQL instance should be set up for high availability (**REGIONAL**) or single zone (**ZONAL**).
- **crash\_safe\_replication** - (Optional) Specific to read instances, indicates when crash-safe replication flags are enabled.
- **disk\_autoresize** - (Optional, Second Generation, Default: **true**) Configuration to increase storage size automatically.
- **disk\_size** - (Optional, Second Generation, Default: 10) The size of data disk, in GB. Size of a running instance cannot be reduced but can be increased.
- **disk\_type** - (Optional, Second Generation, Default: **PD\_SSD**) The type of data disk: **PD\_SSD** or **PD\_HDD**.
- **pricing\_plan** - (Optional, First Generation) Pricing plan for this instance, can be one of **PER\_USE** or **PACKAGE**.
- **replication\_type** - (Optional) Replication type for this instance, can be one of **ASYNCHRONOUS** or **SYNCHRONOUS**.
- **user\_labels** - (Optional) A set of key/value user label pairs to assign to the instance.

The optional **settings.database\_flags** sublist supports:

- **name** - (Optional) Name of the flag.
- **value** - (Optional) Value of the flag.

The optional **settings.backup\_configuration** subblock supports:

- **binary\_log\_enabled** - (Optional) True if binary logging is enabled. If **settings.backup\_configuration.enabled** is false, this must be as well. Cannot be used with Postgres.
- **enabled** - (Optional) True if backup configuration is enabled.
- **start\_time** - (Optional) HH:MM format time indicating when backup configuration starts.

The optional **settings.ip\_configuration** subblock supports:

- **ipv4\_enabled** - (Optional) Whether this Cloud SQL instance should be assigned a public IPV4 address. Either **ipv4\_enabled** must be enabled or a **private\_network** must be configured.
- **private\_network** - (Optional) The VPC network from which the Cloud SQL instance is accessible for private IP. Specifying a network enables private IP. Either **ipv4\_enabled** must be enabled or a **private\_network** must be configured.
- **require\_ssl** - (Optional) True if mysqld should default to **REQUIRE X509** for users connecting over IP.

The optional **settings.ip\_configuration.authorized\_networks[]** sublist supports:

- **expiration\_time** - (Optional) The RFC 3339 formatted date time string indicating when this whitelist expires.
- **name** - (Optional) A name for this whitelist entry.
- **value** - (Optional) A CIDR notation IPv4 or IPv6 address that is allowed to access this instance. Must be set even if other two attributes are not for the whitelist to become active.

The optional **settings.location\_preference** subblock supports:

- **follow\_gae\_application** - (Optional) A GAE application whose zone to remain in. Must be in the same region as this instance.
- **zone** - (Optional) The preferred compute engine zone.

The optional **settings.maintenance\_window** subblock for Second Generation instances declares a one-hour maintenance window when an Instance can automatically restart to apply updates. The maintenance window is specified in UTC time. It supports:

- **day** - (Optional) Day of week (1-7), starting on Monday
- **hour** - (Optional) Hour of day (0-23), ignored if **day** not set
- **update\_track** - (Optional) Receive updates earlier (**canary**) or later (**stable**)

The optional `replica_configuration` block must have `master_instance_name` set to work, cannot be updated, and supports:

- `ca_certificate` - (Optional) PEM representation of the trusted CA's x509 certificate.
- `client_certificate` - (Optional) PEM representation of the slave's x509 certificate.
- `client_key` - (Optional) PEM representation of the slave's private key. The corresponding public key is encoded in the `client_certificate`.
- `connect_retry_interval` - (Optional, Default: 60) The number of seconds between connect retries.
- `dump_file_path` - (Optional) Path to a SQL file in GCS from which slave instances are created. Format is `gs://bucket/filename`.
- `failover_target` - (Optional) Specifies if the replica is the failover target. If the field is set to true the replica will be designated as a failover replica. If the master instance fails, the replica instance will be promoted as the new master instance.
- `master_heartbeat_period` - (Optional) Time in ms between replication heartbeats.
- `password` - (Optional) Password for the replication connection.
- `ssl_cipher` - (Optional) Permissible ciphers for use in SSL encryption.
- `username` - (Optional) Username for replication connection.
- `verify_server_certificate` - (Optional) True if the master's common name value is checked during the SSL handshake.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `self_link` - The URI of the created resource.
- `connection_name` - The connection name of the instance to be used in connection strings. For example, when connecting with Cloud SQL Proxy.
- `service_account_email_address` - The service account email address assigned to the instance. This property is applicable only to Second Generation instances.
- `ip_address.0.ip_address` - The IPv4 address assigned.
- `ip_address.0.time_to_retire` - The time this IP address will be retired, in RFC 3339 format.

- `ip_address.0.type` - The type of this IP address.
  - A **PRIMARY** address is an address that can accept incoming connections.
  - An **OUTGOING** address is the source address of connections originating from the instance, if supported.
  - A **PRIVATE** address is an address for an instance which has been configured to use private networking see: Private IP.
- `first_ip_address` - The first IPv4 address of any type assigned. This is to support accessing the first address in the list in a terraform output when the resource is configured with a `count`.
- `public_ip_address` - The first public (**PRIMARY**) IPv4 address assigned. This is a workaround for an issue fixed in Terraform 0.12 but also provides a convenient way to access an IP of a specific type without performing filtering in a Terraform config.
- `private_ip_address` - The first private (**PRIVATE**) IPv4 address assigned. This is a workaround for an issue fixed in Terraform 0.12 but also provides a convenient way to access an IP of a specific type without performing filtering in a Terraform config.
- `settings.version` - Used to make sure changes to the `settings` block are atomic.
- `server_ca_cert.0.cert` - The CA Certificate used to connect to the SQL Instance via SSL.
- `server_ca_cert.0.common_name` - The CN valid for the CA Cert.
- `server_ca_cert.0.create_time` - Creation time of the CA Cert.
- `server_ca_cert.0.expiration_time` - Expiration time of the CA Cert.
- `server_ca_cert.0.sha1_fingerprint` - SHA Fingerprint of the CA Cert.

## » Timeouts

`google_sql_database_instance` provides the following Timeouts configuration options:

- `create` - Default is 10 minutes.
- `update` - Default is 10 minutes.
- `delete` - Default is 10 minutes.



## » Import

Database instances can be imported using one of any of these accepted formats:

```
$ terraform import google_sql_database_instance.master projects/{{project}}/instances/{{name}}
$ terraform import google_sql_database_instance.master {{project}}/{{name}}
$ terraform import google_sql_database_instance.master {{name}}
```

**NOTE:** Some fields (such as `replica_configuration`) won't show a diff if they are unset in config and set on the server. When importing, double-check that your config has all the fields set that you expect- just seeing no diff isn't sufficient to know that your config could reproduce the imported resource.

## » google\_sql\_ssl\_cert

Creates a new Google SQL SSL Cert on a Google SQL Instance. For more information, see the official documentation, or the JSON API.

**Note:** All arguments including the private key will be stored in the raw state as plain-text. Read more about sensitive data in state.

## » Example Usage

Example creating a SQL Client Certificate.

```
resource "google_sql_database_instance" "master" {
  name = "master-instance"

  settings {
    tier = "D0"
  }
}

resource "google_sql_ssl_cert" "client_cert" {
  common_name = "client-name"
  instance    = "${google_sql_database_instance.master.name}"
}
```

## » Argument Reference

The following arguments are supported:

- **instance** - (Required) The name of the Cloud SQL instance. Changing this forces a new resource to be created.

- **common\_name** - (Required) The common name to be used in the certificate to identify the client. Constrained to [a-zA-Z.-\_]+. Changing this forces a new resource to be created.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **sha1\_fingerprint** - The SHA1 Fingerprint of the certificate.
- **private\_key** - The private key associated with the client certificate.
- **server\_ca\_cert** - The CA cert of the server this client cert was generated from.
- **cert** - The actual certificate data for this client certificate.
- **cert\_serial\_number** - The serial number extracted from the certificate data.
- **create\_time** - The time when the certificate was created in RFC 3339 format, for example 2012-11-15T16:19:00.094Z.
- **expiration\_time** - The time when the certificate expires in RFC 3339 format, for example 2012-11-15T16:19:00.094Z.

## » Import

Since the contents of the certificate cannot be accessed after its creation, this resource cannot be imported.

## » google\_sql\_user

Creates a new Google SQL User on a Google SQL User Instance. For more information, see the official documentation, or the JSON API.

**Note:** All arguments including the username and password will be stored in the raw state as plain-text. Read more about sensitive data in state. Passwords will not be retrieved when running "terraform import".

## » Example Usage

Example creating a SQL User.

```
resource "google_sql_database_instance" "master" {
  name = "master-instance"

  settings {
```

```

        tier = "D0"
    }
}

resource "google_sql_user" "users" {
  name      = "me"
  instance  = "${google_sql_database_instance.master.name}"
  host      = "me.com"
  password  = "changeme"
}

```

## » Argument Reference

The following arguments are supported:

- **instance** - (Required) The name of the Cloud SQL instance. Changing this forces a new resource to be created.
  - **name** - (Required) The name of the user. Changing this forces a new resource to be created.
  - **password** - (Optional) The password for the user. Can be updated.
- 
- **host** - (Optional) The host the user can connect from. This is only supported for MySQL instances. Don't set this field for PostgreSQL instances. Can be an IP address. Changing this forces a new resource to be created.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » Import

SQL users for MySQL databases can be imported using the **project**, **instance**, **host** and **name**, e.g.

```
$ terraform import google_sql_user.users my-project/master-instance/my-domain.com/me
```

SQL users for PostgreSQL databases can be imported using the **project**, **instance** and **name**, e.g.

```
$ terraform import google_sql_user.users my-project/master-instance/me
```

## » google\_logging\_billing\_account\_exclusion

Manages a billing account logging exclusion. For more information see the official documentation and Excluding Logs.

Note that you must have the "Logs Configuration Writer" IAM role (roles/logging.configWriter) granted to the credentials used with Terraform.

### » Example Usage

```
resource "google_logging_billing_account_exclusion" "my-exclusion" {
  name           = "my-instance-debug-exclusion"
  billing_account = "ABCDEF-012345-GHIJKL"

  description = "Exclude GCE instance debug logs"

  # Exclude all DEBUG or lower severity messages relating to instances
  filter = "resource.type = gce_instance AND severity <= DEBUG"
}
```

### » Argument Reference

The following arguments are supported:

- **billing\_account** - (Required) The billing account to create the exclusion for.
- **name** - (Required) The name of the logging exclusion.
- **description** - (Optional) A human-readable description.
- **disabled** - (Optional) Whether this exclusion rule should be disabled or not. This defaults to false.
- **filter** - (Required) The filter to apply when excluding logs. Only log entries that match the filter are excluded. See Advanced Log Filters for information on how to write a filter.

### » Import

Billing account logging exclusions can be imported using their URI, e.g.

```
$ terraform import google_logging_billing_account_exclusion.my_exclusion billingAccounts/my-
```

## » google\_logging\_billing\_account\_sink

Manages a billing account logging sink. For more information see the official documentation and Exporting Logs in the API.

**Note** You must have the "Logs Configuration Writer" IAM role (`roles/logging.configWriter`) granted on the billing account to the credentials used with Terraform. IAM roles granted on a billing account are separate from the typical IAM roles granted on a project.

### » Example Usage

```
resource "google_logging_billing_account_sink" "my-sink" {
  name = "my-sink"
  billing_account = "ABCDEF-012345-GHIJKL"

  # Can export to pubsub, cloud storage, or bigtable
  destination = "storage.googleapis.com/${google_storage_bucket.log-bucket.name}"
}

resource "google_storage_bucket" "log-bucket" {
  name = "billing-logging-bucket"
}

resource "google_project_iam_binding" "log-writer" {
  role = "roles/storage.objectCreator"

  members = [
    "${google_logging_billing_account_sink.my-sink.writer_identity}",
  ]
}
```

### » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the logging sink.
- **billing\_account** - (Required) The billing account exported to the sink.
- **destination** - (Required) The destination of the sink (or, in other words, where logs are written to). Can be a Cloud Storage bucket, a PubSub topic, or a BigQuery dataset. Examples:  
"storage.googleapis.com/[GCS\_BUCKET]" "bigquery.googleapis.com/projects/[PROJECT\_ID]/datasets/[DATASET]"  
"pubsub.googleapis.com/projects/[PROJECT\_ID]/topics/[TOPIC\_ID]"

The writer associated with the sink must have access to write to the above resource.

- **filter** - (Optional) The filter to apply when exporting logs. Only log entries that match the filter are exported. See Advanced Log Filters for information on how to write a filter.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **writer\_identity** - The identity associated with this sink. This identity must be granted write access to the configured **destination**.

## » Import

Billing account logging sinks can be imported using this format:

```
$ terraform import google_logging_billing_account_sink.my_sink billingAccounts/{{billing_account_id}}/sinks/{{sink_name}}
```

## » google\_logging\_folder\_exclusion

Manages a folder-level logging exclusion. For more information see the official documentation and Excluding Logs.

Note that you must have the "Logs Configuration Writer" IAM role (roles/logging.configWriter) granted to the credentials used with Terraform.

## » Example Usage

```
resource "google_logging_folder_exclusion" "my-exclusion" {
  name      = "my-instance-debug-exclusion"
  folder    = "${google_folder.my-folder.name}"

  description = "Exclude GCE instance debug logs"

  # Exclude all DEBUG or lower severity messages relating to instances
  filter      = "resource.type = gce_instance AND severity <= DEBUG"
}

resource "google_folder" "my-folder" {
  name = "my-folder"
```

```

    display_name = "My folder"
    parent       = "organizations/123456"
  }

```

## » Argument Reference

The following arguments are supported:

- **folder** - (Required) The folder to be exported to the sink. Note that either [FOLDER\_ID] or "folders/[FOLDER\_ID]" is accepted.
- **name** - (Required) The name of the logging exclusion.
- **description** - (Optional) A human-readable description.
- **disabled** - (Optional) Whether this exclusion rule should be disabled or not. This defaults to false.
- **filter** - (Required) The filter to apply when excluding logs. Only log entries that match the filter are excluded. See Advanced Log Filters for information on how to write a filter.

## » Import

Folder-level logging exclusions can be imported using their URI, e.g.

```
$ terraform import google_logging_folder_exclusion.my_exclusion folders/my-folder/exclusions
```

## » google\_logging\_folder\_sink

Manages a folder-level logging sink. For more information see the official documentation and Exporting Logs in the API.

Note that you must have the "Logs Configuration Writer" IAM role (roles/logging.configWriter) granted to the credentials used with terraform.

## » Example Usage

```

resource "google_logging_folder_sink" "my-sink" {
  name       = "my-sink"
  folder     = "${google_folder.my-folder.name}"

  # Can export to pubsub, cloud storage, or bigtable
  destination = "storage.googleapis.com/${google_storage_bucket.log-bucket.name}"

```

```

    # Log all WARN or higher severity messages relating to instances
    filter      = "resource.type = gce_instance AND severity >= WARN"
  }

  resource "google_storage_bucket" "log-bucket" {
    name = "folder-logging-bucket"
  }

  resource "google_project_iam_binding" "log-writer" {
    role      = "roles/storage.objectCreator"

    members = [
      "${google_logging_folder_sink.my-sink.writer_identity}",
    ]
  }

  resource "google_folder" "my-folder" {
    display_name = "My folder"
    parent       = "organizations/123456"
  }

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the logging sink.
- **folder** - (Required) The folder to be exported to the sink. Note that either `[FOLDER_ID]` or `"folders/[FOLDER_ID]"` is accepted.
- **destination** - (Required) The destination of the sink (or, in other words, where logs are written to). Can be a Cloud Storage bucket, a PubSub topic, or a BigQuery dataset. Examples: `"storage.googleapis.com/[GCS_BUCKET]"` `"bigquery.googleapis.com/projects/[PROJECT_ID]/datasets/[DATASET]"` `"pubsub.googleapis.com/projects/[PROJECT_ID]/topics/[TOPIC_ID]"` The writer associated with the sink must have access to write to the above resource.
- **filter** - (Optional) The filter to apply when exporting logs. Only log entries that match the filter are exported. See Advanced Log Filters for information on how to write a filter.
- **include\_children** - (Optional) Whether or not to include children folders in the sink export. If true, logs associated with child projects are also exported; otherwise only logs relating to the provided folder are included.



## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **writer\_identity** - The identity associated with this sink. This identity must be granted write access to the configured **destination**.

## » Import

Folder-level logging sinks can be imported using this format:

```
$ terraform import google_logging_folder_sink.my_sink folders/{{folder_id}}/sinks/{{sink_id}}
```

## » google\_logging\_organization\_exclusion

Manages an organization-level logging exclusion. For more information see the official documentation and Excluding Logs.

Note that you must have the "Logs Configuration Writer" IAM role (`roles/logging.configWriter`) granted to the credentials used with Terraform.

## » Example Usage

```
resource "google_logging_organization_exclusion" "my-exclusion" {
  name      = "my-instance-debug-exclusion"
  org_id    = "123456789"

  description = "Exclude GCE instance debug logs"

  # Exclude all DEBUG or lower severity messages relating to instances
  filter      = "resource.type = gce_instance AND severity <= DEBUG"
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the logging exclusion.
- **org\_id** - (Required) The organization to create the exclusion in.
- **description** - (Optional) A human-readable description.

- **disabled** - (Optional) Whether this exclusion rule should be disabled or not. This defaults to false.
- **filter** - (Required) The filter to apply when excluding logs. Only log entries that match the filter are excluded. See Advanced Log Filters for information on how to write a filter.

## » Import

Organization-level logging exclusions can be imported using their URI, e.g.

```
$ terraform import google_logging_organization_exclusion.my_exclusion organizations/my-organ
```

## » google\_logging\_organization\_sink

Manages a organization-level logging sink. For more information see the official documentation and Exporting Logs in the API.

Note that you must have the "Logs Configuration Writer" IAM role (roles/logging.configWriter) granted to the credentials used with terraform.

## » Example Usage

```
resource "google_logging_organization_sink" "my-sink" {
  name      = "my-sink"
  org_id    = "123456789"

  # Can export to pubsub, cloud storage, or bigtable
  destination = "storage.googleapis.com/${google_storage_bucket.log-bucket.name}"

  # Log all WARN or higher severity messages relating to instances
  filter      = "resource.type = gce_instance AND severity >= WARN"
}

resource "google_storage_bucket" "log-bucket" {
  name = "organization-logging-bucket"
}

resource "google_project_iam_binding" "log-writer" {
  role    = "roles/storage.objectCreator"

  members = [
    "${google_logging_organization_sink.my-sink.writer_identity}",
  ]
}
```

```
]
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the logging sink.
- **org\_id** - (Required) The numeric ID of the organization to be exported to the sink.
- **destination** - (Required) The destination of the sink (or, in other words, where logs are written to). Can be a Cloud Storage bucket, a PubSub topic, or a BigQuery dataset. Examples:  
"storage.googleapis.com/[GCS\_BUCKET]" "bigquery.googleapis.com/projects/[PROJECT\_ID]/datasets/[DATASET]"  
"pubsub.googleapis.com/projects/[PROJECT\_ID]/topics/[TOPIC\_ID]"  
The writer associated with the sink must have access to write to the above resource.
- **filter** - (Optional) The filter to apply when exporting logs. Only log entries that match the filter are exported. See Advanced Log Filters for information on how to write a filter.
- **include\_children** - (Optional) Whether or not to include children organizations in the sink export. If true, logs associated with child projects are also exported; otherwise only logs relating to the provided organization are included.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **writer\_identity** - The identity associated with this sink. This identity must be granted write access to the configured **destination**.

## » Import

Organization-level logging sinks can be imported using this format:

```
$ terraform import google_logging_organization_sink.my_sink organizations/{{organization_id}}
```

## » google\_logging\_project\_exclusion

Manages a project-level logging exclusion. For more information see the official documentation and Excluding Logs.

Note that you must have the "Logs Configuration Writer" IAM role (roles/logging.configWriter) granted to the credentials used with Terraform.

### » Example Usage

```
resource "google_logging_project_exclusion" "my-exclusion" {
  name = "my-instance-debug-exclusion"

  description = "Exclude GCE instance debug logs"

  # Exclude all DEBUG or lower severity messages relating to instances
  filter = "resource.type = gce_instance AND severity <= DEBUG"
}
```

### » Argument Reference

The following arguments are supported:

- **filter** - (Required) The filter to apply when excluding logs. Only log entries that match the filter are excluded. See Advanced Log Filters for information on how to write a filter.
- **name** - (Required) The name of the logging exclusion.
- **description** - (Optional) A human-readable description.
- **disabled** - (Optional) Whether this exclusion rule should be disabled or not. This defaults to false.
- **project** - (Optional) The project to create the exclusion in. If omitted, the project associated with the provider is used.

### » Import

Project-level logging exclusions can be imported using their URI, e.g.

```
$ terraform import google_logging_project_exclusion.my_exclusion projects/my-project/exclusion
```

## » google\_logging\_project\_sink

Manages a project-level logging sink. For more information see the official documentation, Exporting Logs in the API and API.

**Note:** You must have granted the "Logs Configuration Writer" IAM role (roles/logging.configWriter) to the credentials used with terraform.

**Note** You must enable the Cloud Resource Manager API

### » Example Usage

```
resource "google_logging_project_sink" "my-sink" {
  name = "my-pubsub-instance-sink"

  # Can export to pubsub, cloud storage, or bigtable
  destination = "pubsub.googleapis.com/projects/my-project/topics/instance-activity"

  # Log all WARN or higher severity messages relating to instances
  filter = "resource.type = gce_instance AND severity >= WARN"

  # Use a unique writer (creates a unique service account used for writing)
  unique_writer_identity = true
}
```

A more complete example follows: this creates a compute instance, as well as a log sink that logs all activity to a cloud storage bucket. Because we are using `unique_writer_identity`, we must grant it access to the bucket. Note that this grant requires the "Project IAM Admin" IAM role (roles/resourcemanager.projectIamAdmin) granted to the credentials used with terraform.

```
# Our logged compute instance
resource "google_compute_instance" "my-logged-instance" {
  name          = "my-instance"
  machine_type  = "n1-standard-1"
  zone          = "us-central1-a"

  boot_disk {
    initialize_params {
      image = "debian-cloud/debian-9"
    }
  }
}

network_interface {
  network = "default"
}
```

```

        access_config {}
    }
}

# A bucket to store logs in
resource "google_storage_bucket" "log-bucket" {
    name      = "my-unique-logging-bucket"
}

# Our sink; this logs all activity related to our "my-logged-instance" instance
resource "google_logging_project_sink" "instance-sink" {
    name = "my-instance-sink"
    destination = "storage.googleapis.com/${google_storage_bucket.log-bucket.name}"
    filter = "resource.type = gce_instance AND resource.labels.instance_id = \"${google_compute_instance.self_link}\""

    unique_writer_identity = true
}

# Because our sink uses a unique_writer, we must grant that writer access to the bucket.
resource "google_project_iam_binding" "log-writer" {
    role = "roles/storage.objectCreator"

    members = [
        "${google_logging_project_sink.instance-sink.writer_identity}",
    ]
}

```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The name of the logging sink.
- **destination** - (Required) The destination of the sink (or, in other words, where logs are written to). Can be a Cloud Storage bucket, a PubSub topic, or a BigQuery dataset. Examples: `"storage.googleapis.com/[GCS_BUCKET]"` `"bigquery.googleapis.com/projects/[PROJECT_ID]/datasets/[DATASET]"` `"pubsub.googleapis.com/projects/[PROJECT_ID]/topics/[TOPIC_ID]"`  
The writer associated with the sink must have access to write to the above resource.
- **filter** - (Optional) The filter to apply when exporting logs. Only log entries that match the filter are exported. See Advanced Log Filters for information on how to write a filter.

- **project** - (Optional) The ID of the project to create the sink in. If omitted, the project associated with the provider is used.
- **unique\_writer\_identity** - (Optional) Whether or not to create a unique identity associated with this sink. If **false** (the default), then the **writer\_identity** used is `serviceAccount:cloud-logs@system.gserviceaccount.com`. If **true**, then a unique service account is created and used for this sink. If you wish to publish logs across projects, you must set **unique\_writer\_identity** to true.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **writer\_identity** - The identity associated with this sink. This identity must be granted write access to the configured **destination**.

## » Import

Project-level logging sinks can be imported using their URI, e.g.

```
$ terraform import google_logging_project_sink.my_sink projects/my-project/sinks/my-sink
```

## » google\_monitoring\_alert\_policy

A description of the conditions under which some aspect of your system is considered to be "unhealthy" and the ways to notify people or services about this state.

To get more information about AlertPolicy, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Monitoring Alert Policy Basic

```
resource "google_monitoring_alert_policy" "alert_policy" {
```

```

display_name = "My Alert Policy"
combiner = "OR"
conditions {
  display_name = "test condition"
  condition_threshold {
    filter = "metric.type=\"compute.googleapis.com/instance/disk/write_bytes_count\" AND r
    duration = "60s"
    comparison = "COMPARISON_GT"
    aggregations {
      alignment_period = "60s"
      per_series_aligner = "ALIGN_RATE"
    }
  }
}
}
}

```

## » Argument Reference

The following arguments are supported:

- **display\_name** - (Required) A short name or phrase used to identify the policy in dashboards, notifications, and incidents. To avoid confusion, don't use the same display name for multiple policies in the same project. The name is limited to 512 Unicode characters.
- **combiner** - (Required) How to combine the results of multiple conditions to determine if an incident should be opened.
- **conditions** - (Required) A list of conditions for the policy. The conditions are combined by AND or OR according to the combiner field. If the combined conditions evaluate to true, then an incident is created. A policy can have from one to six conditions. Structure is documented below.

The **conditions** block supports:

- **condition\_absent** - (Optional) A condition that checks that a time series continues to receive new data points. Structure is documented below.
- **name** - The unique resource name for this condition. Its syntax is: `projects/[PROJECT_ID]/alertPolicies/[POLICY_ID]/conditions/[CONDITION_ID]` [CONDITION\_ID] is assigned by Stackdriver Monitoring when the condition is created as part of a new or updated alerting policy.
- **condition\_threshold** - (Optional) A condition that compares a time series against a threshold. Structure is documented below.
- **display\_name** - (Required) A short name or phrase used to identify the condition in dashboards, notifications, and incidents. To avoid confusion, don't use the same display name for multiple conditions in the same policy.



The `condition_absent` block supports:

- **aggregations** - (Optional) Specifies the alignment of data points in individual time series as well as how to combine the retrieved time series together (such as when aggregating multiple streams on each resource to a single stream for each resource or when aggregating streams across all members of a group of resources). Multiple aggregations are applied in the order specified. Structure is documented below.
- **trigger** - (Optional) The number/percent of time series for which the comparison must hold in order for the condition to trigger. If unspecified, then the condition will trigger if the comparison is true for any of the time series that have been identified by filter and aggregations. Structure is documented below.
- **duration** - (Required) The amount of time that a time series must fail to report new data to be considered failing. Currently, only values that are a multiple of a minute--e.g. 60s, 120s, or 300s --are supported.
- **filter** - (Optional) A filter that identifies which time series should be compared with the threshold. The filter is similar to the one that is specified in the `MetricService.ListTimeSeries` request (that call is useful to verify the time series that will be retrieved / processed) and must specify the metric type and optionally may contain restrictions on resource type, resource labels, and metric labels. This field may not exceed 2048 Unicode characters in length.

The **aggregations** block supports:

- **per\_series\_aligner** - (Optional) The approach to be used to align individual time series. Not all alignment functions may be applied to all time series, depending on the metric type and value type of the original time series. Alignment may change the metric type or the value type of the time series. Time series data must be aligned in order to perform cross- time series reduction. If `crossSeriesReducer` is specified, then `perSeriesAligner` must be specified and not equal `ALIGN_NONE` and `alignmentPeriod` must be specified; otherwise, an error is returned.
- **group\_by\_fields** - (Optional) The set of fields to preserve when `crossSeriesReducer` is specified. The `groupByFields` determine how the time series are partitioned into subsets prior to applying the aggregation function. Each subset contains time series that have the same value for each of the grouping fields. Each individual time series is a member of exactly one subset. The `crossSeriesReducer` is applied to each subset of time series. It is not possible to reduce across different resource types, so this field implicitly contains `resource.type`. Fields not specified in `groupByFields` are aggregated away. If `groupByFields` is not specified and all the time series have the same resource type, then the time series are aggregated into a single output time series. If `crossSeriesReducer` is

not defined, this field is ignored.

- **alignment\_period** - (Optional) The alignment period for per-time series alignment. If present, alignmentPeriod must be at least 60 seconds. After per-time series alignment, each time series will contain data points only on the period boundaries. If perSeriesAligner is not specified or equals ALIGN\_NONE, then this field is ignored. If perSeriesAligner is specified and does not equal ALIGN\_NONE, then this field must be defined; otherwise an error is returned.
- **cross\_series\_reducer** - (Optional) The approach to be used to combine time series. Not all reducer functions may be applied to all time series, depending on the metric type and the value type of the original time series. Reduction may change the metric type of value type of the time series. Time series data must be aligned in order to perform cross- time series reduction. If crossSeriesReducer is specified, then perSeriesAligner must be specified and not equal ALIGN\_NONE and alignmentPeriod must be specified; otherwise, an error is returned.

The **trigger** block supports:

- **percent** - (Optional) The percentage of time series that must fail the predicate for the condition to be triggered.
- **count** - (Optional) The absolute number of time series that must fail the predicate for the condition to be triggered.

The **condition\_threshold** block supports:

- **threshold\_value** - (Optional) A value against which to compare the time series.
- **denominator\_filter** - (Optional) A filter that identifies a time series that should be used as the denominator of a ratio that will be compared with the threshold. If a denominator\_filter is specified, the time series specified by the filter field will be used as the numerator. The filter is similar to the one that is specified in the MetricService.ListTimeSeries request (that call is useful to verify the time series that will be retrieved / processed) and must specify the metric type and optionally may contain restrictions on resource type, resource labels, and metric labels. This field may not exceed 2048 Unicode characters in length.
- **denominator\_aggregations** - (Optional) Specifies the alignment of data points in individual time series selected by denominatorFilter as well as how to combine the retrieved time series together (such as when aggregating multiple streams on each resource to a single stream for each resource or when aggregating streams across all members of a group of resources). When computing ratios, the aggregations and denominator\_aggregations fields must use the same alignment period and produce time series that have the same periodicity and labels. This

field is similar to the one in the `MetricService.ListTimeSeries` request. It is advisable to use the `ListTimeSeries` method when debugging this field. Structure is documented below.

- **duration** - (Required) The amount of time that a time series must violate the threshold to be considered failing. Currently, only values that are a multiple of a minute--e.g., 0, 60, 120, or 300 seconds--are supported. If an invalid value is given, an error will be returned. When choosing a duration, it is useful to keep in mind the frequency of the underlying time series data (which may also be affected by any alignments specified in the aggregations field); a good duration is long enough so that a single outlier does not generate spurious alerts, but short enough that unhealthy states are detected and alerted on quickly.
- **comparison** - (Required) The comparison to apply between the time series (indicated by filter and aggregation) and the threshold (indicated by `threshold_value`). The comparison is applied on each time series, with the time series on the left-hand side and the threshold on the right-hand side. Only `COMPARISON_LT` and `COMPARISON_GT` are supported currently.
- **trigger** - (Optional) The number/percent of time series for which the comparison must hold in order for the condition to trigger. If unspecified, then the condition will trigger if the comparison is true for any of the time series that have been identified by filter and aggregations, or by the ratio, if `denominator_filter` and `denominator_aggregations` are specified. Structure is documented below.
- **aggregations** - (Optional) Specifies the alignment of data points in individual time series as well as how to combine the retrieved time series together (such as when aggregating multiple streams on each resource to a single stream for each resource or when aggregating streams across all members of a group of resources). Multiple aggregations are applied in the order specified. This field is similar to the one in the `MetricService.ListTimeSeries` request. It is advisable to use the `ListTimeSeries` method when debugging this field. Structure is documented below.
- **filter** - (Optional) A filter that identifies which time series should be compared with the threshold. The filter is similar to the one that is specified in the `MetricService.ListTimeSeries` request (that call is useful to verify the time series that will be retrieved / processed) and must specify the metric type and optionally may contain restrictions on resource type, resource labels, and metric labels. This field may not exceed 2048 Unicode characters in length.

The `denominator_aggregations` block supports:

- **per\_series\_aligner** - (Optional) The approach to be used to align individual time series. Not all alignment functions may be applied to all time

series, depending on the metric type and value type of the original time series. Alignment may change the metric type or the value type of the time series. Time series data must be aligned in order to perform cross- time series reduction. If `crossSeriesReducer` is specified, then `perSeriesAligner` must be specified and not equal `ALIGN_NONE` and `alignmentPeriod` must be specified; otherwise, an error is returned.

- **group\_by\_fields** - (Optional) The set of fields to preserve when `crossSeriesReducer` is specified. The `groupByFields` determine how the time series are partitioned into subsets prior to applying the aggregation function. Each subset contains time series that have the same value for each of the grouping fields. Each individual time series is a member of exactly one subset. The `crossSeriesReducer` is applied to each subset of time series. It is not possible to reduce across different resource types, so this field implicitly contains `resource.type`. Fields not specified in `groupByFields` are aggregated away. If `groupByFields` is not specified and all the time series have the same resource type, then the time series are aggregated into a single output time series. If `crossSeriesReducer` is not defined, this field is ignored.
- **alignment\_period** - (Optional) The alignment period for per-time series alignment. If present, `alignmentPeriod` must be at least 60 seconds. After per-time series alignment, each time series will contain data points only on the period boundaries. If `perSeriesAligner` is not specified or equals `ALIGN_NONE`, then this field is ignored. If `perSeriesAligner` is specified and does not equal `ALIGN_NONE`, then this field must be defined; otherwise an error is returned.
- **cross\_series\_reducer** - (Optional) The approach to be used to combine time series. Not all reducer functions may be applied to all time series, depending on the metric type and the value type of the original time series. Reduction may change the metric type of value type of the time series. Time series data must be aligned in order to perform cross- time series reduction. If `crossSeriesReducer` is specified, then `perSeriesAligner` must be specified and not equal `ALIGN_NONE` and `alignmentPeriod` must be specified; otherwise, an error is returned.

The **trigger** block supports:

- **percent** - (Optional) The percentage of time series that must fail the predicate for the condition to be triggered.
- **count** - (Optional) The absolute number of time series that must fail the predicate for the condition to be triggered.

The **aggregations** block supports:

- **per\_series\_aligner** - (Optional) The approach to be used to align individual time series. Not all alignment functions may be applied to all time

series, depending on the metric type and value type of the original time series. Alignment may change the metric type or the value type of the time series. Time series data must be aligned in order to perform cross-time series reduction. If `crossSeriesReducer` is specified, then `perSeriesAligner` must be specified and not equal `ALIGN_NONE` and `alignmentPeriod` must be specified; otherwise, an error is returned.

- **group\_by\_fields** - (Optional) The set of fields to preserve when `crossSeriesReducer` is specified. The `groupByFields` determine how the time series are partitioned into subsets prior to applying the aggregation function. Each subset contains time series that have the same value for each of the grouping fields. Each individual time series is a member of exactly one subset. The `crossSeriesReducer` is applied to each subset of time series. It is not possible to reduce across different resource types, so this field implicitly contains `resource.type`. Fields not specified in `groupByFields` are aggregated away. If `groupByFields` is not specified and all the time series have the same resource type, then the time series are aggregated into a single output time series. If `crossSeriesReducer` is not defined, this field is ignored.
- **alignment\_period** - (Optional) The alignment period for per-time series alignment. If present, `alignmentPeriod` must be at least 60 seconds. After per-time series alignment, each time series will contain data points only on the period boundaries. If `perSeriesAligner` is not specified or equals `ALIGN_NONE`, then this field is ignored. If `perSeriesAligner` is specified and does not equal `ALIGN_NONE`, then this field must be defined; otherwise an error is returned.
- **cross\_series\_reducer** - (Optional) The approach to be used to combine time series. Not all reducer functions may be applied to all time series, depending on the metric type and the value type of the original time series. Reduction may change the metric type or value type of the time series. Time series data must be aligned in order to perform cross-time series reduction. If `crossSeriesReducer` is specified, then `perSeriesAligner` must be specified and not equal `ALIGN_NONE` and `alignmentPeriod` must be specified; otherwise, an error is returned.

- 
- **enabled** - (Optional) Whether or not the policy is enabled. The default is true.
  - **notification\_channels** - (Optional) Identifies the notification channels to which notifications should be sent when incidents are opened or closed or when new violations occur on an already opened incident. Each element of this array corresponds to the name field in each of the `NotificationChannel` objects that are returned from the `notificationChannels.list` method. The syntax of the entries in this field is `projects/[PROJECT_ID]/notificationChannels/[CHANNEL_ID]`

- **labels** - (Optional) User-supplied key/value data to be used for organizing AlertPolicy objects.
- **documentation** - (Optional) A short name or phrase used to identify the policy in dashboards, notifications, and incidents. To avoid confusion, don't use the same display name for multiple policies in the same project. The name is limited to 512 Unicode characters. Structure is documented below.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **documentation** block supports:

- **content** - (Optional) The text of the documentation, interpreted according to mimeType. The content may not exceed 8,192 Unicode characters and may not exceed more than 10,240 bytes when encoded in UTF-8 format, whichever is smaller.
- **mime\_type** - (Optional) The format of the content field. Presently, only the value "text/markdown" is supported.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **name** - The unique resource name for this policy. Its syntax is: projects/[PROJECT\_ID]/alertPolicies/[ALERT\_POLICY\_ID]
- **creation\_record** - A read-only record of the creation of the alerting policy. If provided in a call to create or update, this field will be ignored. Structure is documented below.

The **creation\_record** block contains:

- **mutate\_time** - When the change occurred.
- **mutated\_by** - The email address of the user making the change.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

AlertPolicy can be imported using any of these accepted formats:

```
$ terraform import google_monitoring_alert_policy.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_monitoring\_\_group

The description of a dynamic collection of monitored resources. Each group has a filter that is matched against monitored resources and their associated metadata. If a group's filter matches an available monitored resource, then that resource is a member of that group.

To get more information about Group, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Monitoring Group Basic

```
resource "google_monitoring_group" "basic" {
  display_name = "New Test Group"

  filter = "resource.metadata.region=\"europe-west2\""
}
```



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Monitoring Group Subgroup

```
resource "google_monitoring_group" "parent" {
```

```

    display_name = "New Test SubGroup"
    filter = "resource.metadata.region=\"europe-west2\""
  }

  resource "google_monitoring_group" "subgroup" {
    display_name = "New Test SubGroup"
    filter = "resource.metadata.region=\"europe-west2\""
    parent_name = "${google_monitoring_group.parent.name}"
  }

```

## » Argument Reference

The following arguments are supported:

- **display\_name** - (Required) A user-assigned name for this group, used only for display purposes.
  - **filter** - (Required) The filter used to determine which monitored resources belong to this group.
- 
- **parent\_name** - (Optional) The name of the group's parent, if it has one. The format is "projects/{project\_id\_or\_number}/groups/{group\_id}". For groups with no parent, parentName is the empty string, "".
  - **is\_cluster** - (Optional) If true, the members of this group are considered to be a cluster. The system can perform additional analysis on groups that are clusters.
  - **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **name** - A unique identifier for this group. The format is "projects/{project\_id\_or\_number}/groups/{group\_id}".

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.



## » Import

Group can be imported using any of these accepted formats:

```
$ terraform import google_monitoring_group.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_monitoring\_\_notification\_\_channel

A NotificationChannel is a medium through which an alert is delivered when a policy violation is detected. Examples of channels include email, SMS, and third-party messaging applications. Fields containing sensitive information like authentication tokens or contact info are only partially populated on retrieval.

To get more information about NotificationChannel, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Notification Channel Basic

```
resource "google_monitoring_notification_channel" "basic" {
  display_name = "Test Notification Channel"
  type = "email"
  labels = {
    email_address = "fake_email@blahblah.com"
  }
}
```

## » Argument Reference

The following arguments are supported:

- **type** - (Required) The type of the notification channel. This field matches the value of the NotificationChannelDescriptor.type field. See [https://cloud.google.com/monitoring/api/ref\\_v3/rest/v3/projects](https://cloud.google.com/monitoring/api/ref_v3/rest/v3/projects).

notificationChannelDescriptors/list to get the list of valid values such as "email", "slack", etc...

- **display\_name** - (Required) An optional human-readable name for this notification channel. It is recommended that you specify a non-empty and unique name in order to make it easier to identify the channels in your project, though this is not enforced. The display name is limited to 512 Unicode characters.

- 
- **labels** - (Optional) Configuration fields that define the channel and its behavior. The permissible and required labels are specified in the NotificationChannelDescriptor corresponding to the type field. **Note:** Some NotificationChannelDescriptor labels are sensitive and the API will return an partially-obfuscated value. For example, for "type": "slack" channels, an **auth\_token** label with value "SECRET" will be obfuscated as "\*\*\*CRET". In order to avoid a diff, Terraform will use the state value if it appears that the obfuscated value matches the state value in length/unobfuscated characters. However, Terraform will not detect a diff if the obfuscated portion of the value was changed outside of Terraform.

- **user\_labels** - (Optional) User-supplied key/value data that does not need to conform to the corresponding NotificationChannelDescriptor's schema, unlike the labels field. This field is intended to be used for organizing and identifying the NotificationChannel objects. The field can contain up to 64 entries. Each key and value is limited to 63 Unicode characters or 128 bytes, whichever is smaller. Labels and values can contain only lowercase letters, numerals, underscores, and dashes. Keys must begin with a letter.

- **description** - (Optional) An optional human-readable description of this notification channel. This description may provide additional details, beyond the display name, for the channel. This may not exceed 1024 Unicode characters.

- **enabled** - (Optional) Whether notifications are forwarded to the described channel. This makes it possible to disable delivery of notifications to a particular channel without removing the channel from all alerting policies that reference the channel. This is a more convenient approach when the change is temporary and you want to receive notifications from the same set of alerting policies on the channel at some point in the future.

- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **name** - The full REST resource name for this channel. The syntax is: `projects/[PROJECT_ID]/notificationChannels/[CHANNEL_ID]`. The `[CHANNEL_ID]` is automatically assigned by the server on creation.
- **verification\_status** - Indicates whether this channel has been verified or not. On a `ListNotificationChannels` or `GetNotificationChannel` operation, this field is expected to be populated. If the value is `UNVERIFIED`, then it indicates that the channel is non-functioning (it both requires verification and lacks verification); otherwise, it is assumed that the channel works. If the channel is neither `VERIFIED` nor `UNVERIFIED`, it implies that the channel is of a type that does not require verification or that this specific channel has been exempted from verification because it was created prior to verification being required for channels of this type. This field cannot be modified using a standard `UpdateNotificationChannel` operation. To change the value of this field, you must call `VerifyNotificationChannel`.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

`NotificationChannel` can be imported using any of these accepted formats:

```
$ terraform import google_monitoring_notification_channel.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_monitoring_uptime_check_config`

This message configures which resources and services to monitor for availability.

To get more information about `UptimeCheckConfig`, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

### » Example Usage - Uptime Check Config Http

```
resource "google_monitoring_uptime_check_config" "http" {
  display_name = "http-uptime-check"
  timeout = "60s"

  http_check {
    path = "/some-path"
    port = "8010"
  }

  monitored_resource {
    type = "uptime_url"
    labels = {
      project_id = "example"
      host = "192.168.1.1"
    }
  }

  content_matchers {
    content = "example"
  }
}
```



OPEN IN GOOGLE CLOUD SHELL

### » Example Usage - Uptime Check Tcp

```
resource "google_monitoring_uptime_check_config" "tcp_group" {
  display_name = "tcp-uptime-check"
  timeout = "60s"
```

```

tcp_check {
  port = 888
}

resource_group {
  resource_type = "INSTANCE"
  group_id = "${google_monitoring_group.check.name}"
}

resource "google_monitoring_group" "check" {
  display_name = "uptime-check-group"
  filter = "resource.metadata.name=has_substring(\"foo\")"
}

```

## » Argument Reference

The following arguments are supported:

- **display\_name** - (Required) A human-friendly name for the uptime check configuration. The display name should be unique within a Stackdriver Workspace in order to make it easier to identify; however, uniqueness is not enforced.
  - **timeout** - (Required) The maximum amount of time to wait for the request to complete (must be between 1 and 60 seconds). Accepted formats <https://developers.google.com/protocol-buffers/docs/reference/google.protobuf#google.protobuf.Duration>
- 
- **period** - (Optional) How often, in seconds, the uptime check is performed. Currently, the only supported values are 60s (1 minute), 300s (5 minutes), 600s (10 minutes), and 900s (15 minutes). Optional, defaults to 300s.
  - **content\_matchers** - (Optional) The expected content on the page the check is run against. Currently, only the first entry in the list is supported, and other entries will be ignored. The server will look for an exact match of the string in the page response's content. This field is optional and should only be specified if a content match is required. Structure is documented below.
  - **selected\_regions** - (Optional) The list of regions from which the check will be run. Some regions contain one location, and others contain more than one. If this field is specified, enough regions to include a minimum of 3 locations must be provided, or an error message is returned. Not specifying this field will result in uptime checks running from all regions.

- **is\_internal** - (Optional) If this is true, then checks are made only from the 'internal\_checkers'. If it is false, then checks are made only from the 'selected\_regions'. It is an error to provide 'selected\_regions' when is\_internal is true, or to provide 'internal\_checkers' when is\_internal is false.
- **internal\_checkers** - (Optional) The internal checkers that this check will egress from. If is\_internal is true and this list is empty, the check will egress from all the InternalCheckers configured for the project that owns this CheckConfig. Structure is documented below.
- **http\_check** - (Optional) Contains information needed to make an HTTP or HTTPS check. Structure is documented below.
- **tcp\_check** - (Optional) Contains information needed to make a TCP check. Structure is documented below.
- **resource\_group** - (Optional) The group resource associated with the configuration. Structure is documented below.
- **monitored\_resource** - (Optional) The monitored resource (<https://cloud.google.com/monitoring/api/resources>) associated with the configuration. The following monitored resource types are supported for uptime checks: `uptime_url` `gce_instance` `gae_app` `aws_ec2_instance` `aws_elb_load_balancer` Structure is documented below.
- **project** - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.

The **content\_matchers** block supports:

- **content** - (Optional) String or regex content to match (max 1024 bytes)

The **internal\_checkers** block supports:

- **gcp\_zone** - (Optional) The GCP zone the uptime check should egress from. Only respected for internal uptime checks, where internal\_network is specified.
- **peer\_project\_id** - (Optional) The GCP project\_id where the internal checker lives. Not necessary the same as the workspace project.
- **name** - (Optional) A unique resource name for this InternalChecker. The format is `projects/[PROJECT_ID]/internalCheckers/[INTERNAL_CHECKER_ID]`. `PROJECT_ID` is the stackdriver workspace project for the uptime check config associated with the internal checker.
- **network** - (Optional) The GCP VPC network (<https://cloud.google.com/vpc/docs/vpc>) where the internal resource lives (ex: "default").
- **display\_name** - (Optional) The checker's human-readable name. The display name should be unique within a Stackdriver Workspace in order to make it easier to identify; however, uniqueness is not enforced.

The `http_check` block supports:

- **auth\_info** - (Optional) The authentication information. Optional when creating an HTTP check; defaults to empty. Structure is documented below.
- **port** - (Optional) The port to the page to run the check against. Will be combined with host (specified within the `MonitoredResource`) and path to construct the full URL. Optional (defaults to 80 without SSL, or 443 with SSL).
- **headers** - (Optional) The list of headers to send as part of the uptime check request. If two headers have the same key and different values, they should be entered as a single header, with the value being a comma-separated list of all the desired values as described at <https://www.w3.org/Protocols/rfc2616/rfc2616.txt> (page 31). Entering two separate headers with the same key in a Create call will cause the first to be overwritten by the second. The maximum number of headers allowed is 100.
- **path** - (Optional) The path to the page to run the check against. Will be combined with the host (specified within the `MonitoredResource`) and port to construct the full URL. Optional (defaults to `"/"`).
- **use\_ssl** - (Optional) If true, use HTTPS instead of HTTP to run the check.
- **mask\_headers** - (Optional) Boolean specifying whether to encrypt the header information. Encryption should be specified for any headers related to authentication that you do not wish to be seen when retrieving the configuration. The server will be responsible for encrypting the headers. On Get/List calls, if `mask_headers` is set to True then the headers will be obscured with `*****`.

The `auth_info` block supports:

- **password** - (Optional) The password to authenticate.
- **username** - (Optional) The username to authenticate.

The `tcp_check` block supports:

- **port** - (Required) The port to the page to run the check against. Will be combined with host (specified within the `MonitoredResource`) to construct the full URL.

The `resource_group` block supports:

- **resource\_type** - (Optional) The resource type of the group members.
- **group\_id** - (Optional) The group of resources being monitored. Should be the `name` of a group

The `monitored_resource` block supports:

- **type** - (Required) The monitored resource type. This field must match the type field of a MonitoredResourceDescriptor ([https://cloud.google.com/monitoring/api/ref\\_v3/rest/v3/projects.monitoredResourceDescriptors#MonitoredResourceDescriptor](https://cloud.google.com/monitoring/api/ref_v3/rest/v3/projects.monitoredResourceDescriptors#MonitoredResourceDescriptor)) object. For example, the type of a Compute Engine VM instance is gce\_instance. For a list of types, see Monitoring resource types (<https://cloud.google.com/monitoring/api/resources>) and Logging resource types (<https://cloud.google.com/logging/docs/api/v2/resource-list>).
- **labels** - (Required) Values for all of the labels listed in the associated monitored resource descriptor. For example, Compute Engine VM instances use the labels "project\_id", "instance\_id", and "zone".

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **name** - A unique resource name for this UptimeCheckConfig. The format is projects/[PROJECT\_ID]/uptimeCheckConfigs/[UPTIME\_CHECK\_ID].
- **uptime\_check\_id** - The id of the uptime check

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

UptimeCheckConfig can be imported using any of these accepted formats:

```
$ terraform import google_monitoring_uptime_check_config.default {{name}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_\_storage\_\_bucket

Creates a new bucket in Google cloud storage service (GCS). Once a bucket has been created, its location can't be changed. ACLs can be applied using the



`google_storage_bucket_acl` resource.

For more information see the official documentation and API.

**Note:** When importing a bucket or using only the default provider project for bucket creation, you will need to enable the Compute API and will otherwise get an error with a link to the API enablement page. If you would prefer not to enable the Compute API, make sure to explicitly set `project` on the bucket resource.

## » Example Usage

Example creating a private bucket in standard storage, in the EU region.

```
resource "google_storage_bucket" "image-store" {
  name      = "image-store-bucket"
  location  = "EU"

  website {
    main_page_suffix = "index.html"
    not_found_page   = "404.html"
  }
}
```

## » Argument Reference

The following arguments are supported:

- `name` - (Required) The name of the bucket.
- 
- `force_destroy` - (Optional, Default: `false`) When deleting a bucket, this boolean option will delete all contained objects. If you try to delete a bucket that contains objects, Terraform will fail that run.
  - `location` - (Optional, Default: `'US'`) The GCS location
  - `project` - (Optional) The ID of the project in which the resource belongs. If it is not provided, the provider project is used.
  - `storage_class` - (Optional) The Storage Class of the new bucket. Supported values include: `MULTI_REGIONAL`, `REGIONAL`, `NEARLINE`, `COLDLINE`.
  - `lifecycle_rule` - (Optional) The bucket's Lifecycle Rules configuration. Multiple blocks of this type are permitted. Structure is documented below.
  - `versioning` - (Optional) The bucket's Versioning configuration.

- **website** - (Optional) Configuration if the bucket acts as a website. Structure is documented below.
- **cors** - (Optional) The bucket's Cross-Origin Resource Sharing (CORS) configuration. Multiple blocks of this type are permitted. Structure is documented below.
- **labels** - (Optional) A set of key/value label pairs to assign to the bucket.
- **logging** - (Optional) The bucket's Access & Storage Logs configuration.
- **encryption** - (Optional) The bucket's encryption configuration.
- **requester\_pays** - (Optional, Default: false) Enables Requester Pays on a storage bucket.

The **lifecycle\_rule** block supports:

- **action** - (Required) The Lifecycle Rule's action configuration. A single block of this type is supported. Structure is documented below.
- **condition** - (Required) The Lifecycle Rule's condition configuration. A single block of this type is supported. Structure is documented below.

The **action** block supports:

- **type** - The type of the action of this Lifecycle Rule. Supported values include: **Delete** and **SetStorageClass**.
- **storage\_class** - (Required if action type is **SetStorageClass**) The target Storage Class of objects affected by this Lifecycle Rule. Supported values include: **MULTI\_REGIONAL**, **REGIONAL**, **NEARLINE**, **COLDLINE**.

The **condition** block supports the following elements, and requires at least one to be defined:

- **age** - (Optional) Minimum age of an object in days to satisfy this condition.
- **created\_before** - (Optional) Creation date of an object in RFC 3339 (e.g. 2017-06-13) to satisfy this condition.
- **is\_live** - (Optional) Defaults to **false** to match archived objects. If **true**, this condition matches live objects. Unversioned buckets have only live objects.
- **matches\_storage\_class** - (Optional) Storage Class of objects to satisfy this condition. Supported values include: **MULTI\_REGIONAL**, **REGIONAL**, **NEARLINE**, **COLDLINE**, **STANDARD**, **DURABLE\_REDUCED\_AVAILABILITY**.
- **num\_newer\_versions** - (Optional) Relevant only for versioned objects. The number of newer versions of an object to satisfy this condition.

The **versioning** block supports:

- **enabled** - (Optional) While set to **true**, versioning is fully enabled for this bucket.

The **website** block supports:

- **main\_page\_suffix** - (Optional) Behaves as the bucket's directory index where missing objects are treated as potential directories.
- **not\_found\_page** - (Optional) The custom object to return when a requested resource is not found.

The **cors** block supports:

- **origin** - (Optional) The list of Origins eligible to receive CORS response headers. Note: "\*" is permitted in the list of origins, and means "any Origin".
- **method** - (Optional) The list of HTTP methods on which to include CORS response headers, (GET, OPTIONS, POST, etc) Note: "\*" is permitted in the list of methods, and means "any method".
- **response\_header** - (Optional) The list of HTTP headers other than the simple response headers to give permission for the user-agent to share across domains.
- **max\_age\_seconds** - (Optional) The value, in seconds, to return in the Access-Control-Max-Age header used in preflight responses.

The **logging** block supports:

- **log\_bucket** - (Required) The bucket that will receive log objects.
- **log\_object\_prefix** - (Optional, Computed) The object prefix for log objects. If it's not provided, by default GCS sets this to this bucket's name.

The **encryption** block supports:

- **default\_kms\_key\_name**: A Cloud KMS key that will be used to encrypt objects inserted into this bucket, if no encryption method is specified. You must pay attention to whether the crypto key is available in the location that this bucket is created in. See the docs for more details.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **self\_link** - The URI of the created resource.
- **url** - The base URL of the bucket, in the format **gs://<bucket-name>**.

## » Import

Storage buckets can be imported using the **name**, e.g.

```
$ terraform import google_storage_bucket.image-store image-store-bucket
```

## » google\_\_storage\_\_bucket\_\_acl

Creates a new bucket ACL in Google cloud storage service (GCS). For more information see the official documentation and API.

## » Example Usage

Example creating an ACL on a bucket with one owner, and one reader.

```
resource "google_storage_bucket" "image-store" {
  name      = "image-store-bucket"
  location = "EU"
}

resource "google_storage_bucket_acl" "image-store-acl" {
  bucket = "${google_storage_bucket.image-store.name}"

  role_entity = [
    "OWNER:user-my.email@gmail.com",
    "READER:group-mygroup",
  ]
}
```

## » Argument Reference

- **bucket** - (Required) The name of the bucket it applies to.
- 
- **predefined\_acl** - (Optional) The canned GCS ACL to apply. Must be set if **role\_entity** is not.
  - **role\_entity** - (Optional) List of role/entity pairs in the form **ROLE:entity**. See GCS Bucket ACL documentation for more details. Must be set if **predefined\_acl** is not.
  - **default\_acl** - (Optional) Configure this ACL to be the default ACL.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » IAM policy for Google storage bucket

Three different resources help you manage your IAM policy for storage bucket. Each of these resources serves a different use case:

- `google_storage_bucket_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the storage bucket are preserved.
- `google_storage_bucket_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the storage bucket are preserved.
- `google_storage_bucket_iam_policy`: Setting a policy removes all other permissions on the bucket, and if done incorrectly, there's a real chance you will lock yourself out of the bucket. If possible for your use case, using multiple `google_storage_bucket_iam_binding` resources will be much safer. See the usage example on how to work with policy correctly.

**Note:** `google_storage_bucket_iam_binding` resources **can be** used in conjunction with `google_storage_bucket_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_storage_bucket_iam_binding`

```
resource "google_storage_bucket_iam_binding" "binding" {
  bucket = "your-bucket-name"
  role   = "roles/storage.objectViewer"

  members = [
    "user:jane@example.com",
  ]
}
```

### » `google_storage_bucket_iam_member`

```
resource "google_storage_bucket_iam_member" "member" {
  bucket = "your-bucket-name"
  role   = "roles/storage.objectViewer"
  member = "user:jane@example.com"
}
```

## » google\_storage\_bucket\_iam\_policy

When applying a policy that does not include the roles listed below, you lose the default permissions which google adds to your bucket: `*roles/storage.legacyBucketOwner * roles/storage.legacyBucketReader`

If this happens only an entity with `roles/storage.admin` privileges can repair this bucket's policies. It is recommended to include the above roles in policies to get the same behaviour as with the other two options.

```
data "google_iam_policy" "foo-policy" {
  binding {
    role = "roles/your-role"

    members = [ "group:yourgroup@example.com" ]
  }
}

resource "google_storage_bucket_iam_policy" "member" {
  bucket = "your-bucket-name"
  policy_data = "${data.google_iam_policy.foo-policy.policy_data}"
}
```

## » Argument Reference

The following arguments are supported:

- **bucket** - (Required) The name of the bucket it applies to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.

- **role** - (Required) The role that should be applied. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the storage bucket's IAM policy.

## » IAM policy for Google storage bucket

Three different resources help you manage your IAM policy for storage bucket. Each of these resources serves a different use case:

- **google\_storage\_bucket\_iam\_binding**: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the storage bucket are preserved.
- **google\_storage\_bucket\_iam\_member**: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the storage bucket are preserved.
- **google\_storage\_bucket\_iam\_policy**: Setting a policy removes all other permissions on the bucket, and if done incorrectly, there's a real chance you will lock yourself out of the bucket. If possible for your use case, using multiple `google_storage_bucket_iam_binding` resources will be much safer. See the usage example on how to work with policy correctly.

**Note:** `google_storage_bucket_iam_binding` resources **can be** used in conjunction with `google_storage_bucket_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_storage_bucket_iam_binding`

```
resource "google_storage_bucket_iam_binding" "binding" {
  bucket = "your-bucket-name"
  role    = "roles/storage.objectViewer"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_storage\_bucket\_iam\_member

```
resource "google_storage_bucket_iam_member" "member" {
  bucket = "your-bucket-name"
  role   = "roles/storage.objectViewer"
  member = "user:jane@example.com"
}
```

## » google\_storage\_bucket\_iam\_policy

When applying a policy that does not include the roles listed below, you lose the default permissions which google adds to your bucket: `*roles/storage.legacyBucketOwner` \* `roles/storage.legacyBucketReader`

If this happens only an entity with `roles/storage.admin` privileges can repair this bucket's policies. It is recommended to include the above roles in policies to get the same behaviour as with the other two options.

```
data "google_iam_policy" "foo-policy" {
  binding {
    role = "roles/your-role"

    members = [ "group:yourgroup@example.com" ]
  }
}

resource "google_storage_bucket_iam_policy" "member" {
  bucket = "your-bucket-name"
  policy_data = "${data.google_iam_policy.foo-policy.policy_data}"
}
```

## » Argument Reference

The following arguments are supported:

- **bucket** - (Required) The name of the bucket it applies to.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.



- **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
- **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
- **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the storage bucket's IAM policy.

## » google\_storage\_bucket\_object

Creates a new object inside an existing bucket in Google cloud storage service (GCS). ACLs can be applied using the `google_storage_object_acl` resource. For more information see the official documentation and API.

## » Example Usage

Example creating a public object in an existing `image-store` bucket.

```
resource "google_storage_bucket_object" "picture" {
  name     = "butterfly01"
  source   = "/images/nature/garden-tiger-moth.jpg"
  bucket   = "image-store"
}
```

## » Argument Reference

The following arguments are supported:

- **bucket** - (Required) The name of the containing bucket.
- **name** - (Required) The name of the object. If you're interpolating the name of this object, see `output_name` instead.

One of the following is required:

- **content** - (Optional) Data as **string** to be uploaded. Must be defined if **source** is not.
  - **source** - (Optional) A path to the data you want to upload. Must be defined if **content** is not.
- 
- **cache\_control** - (Optional) Cache-Control directive to specify caching behavior of object data. If omitted and object is accessible to all anonymous users, the default will be public, max-age=3600
  - **content\_disposition** - (Optional) Content-Disposition of the object data.
  - **content\_encoding** - (Optional) Content-Encoding of the object data.
  - **content\_language** - (Optional) Content-Language of the object data.
  - **content\_type** - (Optional) Content-Type of the object data. Defaults to "application/octet-stream" or "text/plain; charset=utf-8".
  - **storage\_class** - (Optional) The StorageClass of the new bucket object. Supported values include: **MULTI\_REGIONAL**, **REGIONAL**, **NEARLINE**, **COLDLINE**. If not provided, this defaults to the bucket's default storage class or to a standard class.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **crc32c** - (Computed) Base 64 CRC32 hash of the uploaded data.
- **md5hash** - (Computed) Base 64 MD5 hash of the uploaded data.
- **self\_link** - (Computed) A url reference to this object.
- **output\_name** - (Computed) The name of the object. Use this field in interpolations with `google_storage_object_acl` to recreate `google_storage_object_acl` resources when your `google_storage_bucket_object` is recreated.

## » `google_storage_default_object_access_control`

The `DefaultObjectAccessControls` resources represent the Access Control Lists (ACLs) applied to a new object within a Google Cloud Storage bucket when no

ACL was provided for that object. ACLs let you specify who has access to your bucket contents and to what extent.

There are two roles that can be assigned to an entity:

READERs can get an object, though the acl property will not be revealed. OWNERs are READERs, and they can get the acl property, update an object, and call all objectAccessControls methods on the object. The owner of an object is always an OWNER. For more information, see Access Control, with the caveat that this API uses READER and OWNER instead of READ and FULL\_CONTROL.

To get more information about DefaultObjectAccessControl, see:

- API documentation
- How-to Guides
  - Official Documentation



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Storage Default Object Access Control Public

```
resource "google_storage_default_object_access_control" "public_rule" {
  bucket = "${google_storage_bucket.bucket.name}"
  role   = "READER"
  entity = "allUsers"
}

resource "google_storage_bucket" "bucket" {
  name = "static-content-bucket"
}
```

## » Argument Reference

The following arguments are supported:

- **bucket** - (Required) The name of the bucket.
- **entity** - (Required) The entity holding the permission, in one of the following forms:
  - user-{{userId}}
  - user-{{email}} (such as "user-liz@example.com")

- group-{{groupId}}
  - group-{{email}} (such as "group-example@googlegroups.com")
  - domain-{{domain}} (such as "domain-example.com")
  - project-team-{{projectId}}
  - allUsers
  - allAuthenticatedUsers
- **role** - (Required) The access permission for the entity.
- 
- **object** - (Optional) The name of the object, if applied to an object.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **domain** - The domain associated with the entity.
- **email** - The email address associated with the entity.
- **entity\_id** - The ID for the entity
- **generation** - The content generation of the object, if applied to an object.
- **project\_team** - The project team associated with the entity Structure is documented below.

The **project\_team** block contains:

- **project\_number** - (Optional) The project team associated with the entity
- **team** - (Optional) The team.

## » Timeouts

This resource provides the following Timeouts configuration options:

- **create** - Default is 4 minutes.
- **update** - Default is 4 minutes.
- **delete** - Default is 4 minutes.

## » Import

DefaultObjectAccessControl can be imported using any of these accepted formats:

```
$ terraform import google_storage_default_object_access_control.default {{bucket}}/{{entity}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » `google_storage_default_object_acl`

Authoritatively manages the default object ACLs for a Google Cloud Storage bucket without managing the bucket itself.

Note that for each object, its creator will have the "OWNER" role in addition to the default ACL that has been defined.

For more information see the official documentation and API.

Want fine-grained control over default object ACLs? Use `google_storage_default_object_access_control` to control individual role entity pairs.

### » Example Usage

Example creating a default object ACL on a bucket with one owner, and one reader.

```
resource "google_storage_bucket" "image-store" {
  name      = "image-store-bucket"
  location = "EU"
}

resource "google_storage_default_object_acl" "image-store-default-acl" {
  bucket = "${google_storage_bucket.image-store.name}"
  role_entity = [
    "OWNER:user-my.email@gmail.com",
    "READER:group-mygroup",
  ]
}
```

### » Argument Reference

- `bucket` - (Required) The name of the bucket it applies to.
- 
- `role_entity` - (Optional) List of role/entity pairs in the form `ROLE:entity`. See GCS Object ACL documentation for more details. Omitting the field is the same as providing an empty list.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » `google_storage_notification`

Creates a new notification configuration on a specified bucket, establishing a flow of event notifications from GCS to a Cloud Pub/Sub topic. For more information see the official documentation and API.

In order to enable notifications, a special Google Cloud Storage service account unique to the project must have the IAM permission `projects.topics.publish` for a Cloud Pub/Sub topic in the project. To get the service account's email address, use the `google_storage_project_service_account` datasource's `email_address` value, and see below for an example of enabling notifications by granting the correct IAM permission. See the notifications documentation for more details.

## » Example Usage

```
resource "google_storage_notification" "notification" {
  bucket          = "${google_storage_bucket.bucket.name}"
  payload_format   = "JSON_API_V1"
  topic           = "${google_pubsub_topic.topic.id}"
  event_types      = ["OBJECT_FINALIZE", "OBJECT_METADATA_UPDATE"]
  custom_attributes = {
    new-attribute = "new-attribute-value"
  }
  depends_on      = ["google_pubsub_topic_iam_binding.binding"]
}
```

```
// Enable notifications by giving the correct IAM permission to the unique service account.
```

```
data "google_storage_project_service_account" "gcs_account" {}
```

```
resource "google_pubsub_topic_iam_binding" "binding" {
  topic      = "${google_pubsub_topic.topic.name}"
  role       = "roles/pubsub.publisher"
  members    = ["serviceAccount:${data.google_storage_project_service_account.gcs_account}"]
}
```

```
// End enabling notifications
```

```

resource "google_storage_bucket" "bucket" {
  name = "default_bucket"
}

resource "google_pubsub_topic" "topic" {
  name = "default_topic"
}

```

## » Argument Reference

The following arguments are supported:

- **bucket** - (Required) The name of the bucket.
  - **payload\_format** - (Required) The desired content of the Payload. One of "JSON\_API\_V1" or "NONE".
  - **topic** - (Required) The Cloud PubSub topic to which this subscription publishes. Expects either the topic name, assumed to belong to the default GCP provider project, or the project-level name, i.e. `projects/my-gcp-project/topics/my-topic` or `my-topic`.
- 
- **custom\_attributes** - (Optional) A set of key/value attribute pairs to attach to each Cloud PubSub message published for this notification subscription
  - **event\_types** - (Optional) List of event type filters for this notification config. If not specified, Cloud Storage will send notifications for all event types. The valid types are: "OBJECT\_FINALIZE", "OBJECT\_METADATA\_UPDATE", "OBJECT\_DELETE", "OBJECT\_ARCHIVE"
  - **object\_name\_prefix** - (Optional) Specifies a prefix path filter for this notification config. Cloud Storage will only send notifications for objects in this bucket whose names begin with the specified prefix.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **self\_link** - The URI of the created resource.

## » Import

Storage notifications can be imported using the notification id in the format `<bucket_name>/notificationConfigs/<id>` e.g.

```
$ terraform import google_storage_notification.notification default_bucket/notificationConf
```

## » google\_storage\_object\_access\_control

The `ObjectAccessControls` resources represent the Access Control Lists (ACLs) for objects within Google Cloud Storage. ACLs let you specify who has access to your data and to what extent.

There are two roles that can be assigned to an entity:

`READERS` can get an object, though the `acl` property will not be revealed. `OWNERS` are `READERS`, and they can get the `acl` property, update an object, and call all `objectAccessControls` methods on the object. The owner of an object is always an `OWNER`. For more information, see [Access Control](#), with the caveat that this API uses `READER` and `OWNER` instead of `READ` and `FULL_CONTROL`.

To get more information about `ObjectAccessControl`, see:

- [API documentation](#)
- [How-to Guides](#)
  - [Official Documentation](#)



OPEN IN GOOGLE CLOUD SHELL

## » Example Usage - Storage Object Access Control Public Object

```
resource "google_storage_object_access_control" "public_rule" {
  object = "${google_storage_bucket_object.object.output_name}"
  bucket = "${google_storage_bucket.bucket.name}"
  role   = "READER"
  entity = "allUsers"
}
```

```
resource "google_storage_bucket" "bucket" {
  name = "static-content-bucket"
```



```

}

resource "google_storage_bucket_object" "object" {
  name     = "public-object"
  bucket   = "${google_storage_bucket.bucket.name}"
  source   = "../static/img/header-logo.png"
}

```

## » Argument Reference

The following arguments are supported:

- **bucket** - (Required) The name of the bucket.
  - **entity** - (Required) The entity holding the permission, in one of the following forms:
    - user-**{{userId}}**
    - user-**{{email}}** (such as "user-liz@example.com")
    - group-**{{groupId}}**
    - group-**{{email}}** (such as "group-example@googlegroups.com")
    - domain-**{{domain}}** (such as "domain-example.com")
    - project-team-**{{projectId}}**
    - allUsers
    - allAuthenticatedUsers
  - **object** - (Required) The name of the object to apply the access control to.
  - **role** - (Required) The access permission for the entity.
- 

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **domain** - The domain associated with the entity.
- **email** - The email address associated with the entity.
- **entity\_id** - The ID for the entity
- **generation** - The content generation of the object, if applied to an object.
- **project\_team** - The project team associated with the entity Structure is documented below.

The **project\_team** block contains:

- `project_number` - (Optional) The project team associated with the entity
- `team` - (Optional) The team.

## » Timeouts

This resource provides the following Timeouts configuration options:

- `create` - Default is 4 minutes.
- `update` - Default is 4 minutes.
- `delete` - Default is 4 minutes.

## » Import

ObjectAccessControl can be imported using any of these accepted formats:

```
$ terraform import google_storage_object_access_control.default {{bucket}}/{{object}}/{{entity}}
```

If you're importing a resource with beta features, make sure to include `-provider=google-beta` as an argument so that Terraform uses the correct provider to import your resource.

## » google\_storage\_object\_acl

Authoritatively manages the access control list (ACL) for an object in a Google Cloud Storage (GCS) bucket. Removing a `google_storage_object_acl` sets the acl to the `private` predefined ACL.

For more information see the official documentation and API.

Want fine-grained control over object ACLs? Use `google_storage_object_access_control` to control individual role entity pairs.

## » Example Usage

Create an object ACL with one owner and one reader.

```
resource "google_storage_bucket" "image-store" {
  name      = "image-store-bucket"
  location = "EU"
}

resource "google_storage_bucket_object" "image" {
  name      = "image1"
  bucket    = "${google_storage_bucket.image-store.name}"
}
```

```

    source = "image1.jpg"
  }

resource "google_storage_object_acl" "image-store-acl" {
  bucket = "${google_storage_bucket.image-store.name}"
  object = "${google_storage_bucket_object.image.output_name}"

  role_entity = [
    "OWNER:user-my.email@gmail.com",
    "READER:group-mygroup",
  ]
}

```

## » Argument Reference

- `bucket` - (Required) The name of the bucket the object is stored in.
  - `object` - (Required) The name of the object to apply the acl to.
- 
- `predefined_acl` - (Optional) The "canned" predefined ACL to apply. Must be set if `role_entity` is not.
  - `role_entity` - (Optional) List of role/entity pairs in the form `ROLE:entity`. See GCS Object ACL documentation for more details. Must be set if `predefined_acl` is not.

The object's creator will always have `OWNER` permissions for their object, and any attempt to modify that permission would return an error. Instead, Terraform automatically adds that role/entity pair to your `terraform plan` results when it is omitted in your config; `terraform plan` will show the correct final state at every point except for at `Create` time, where the object role/entity pair is omitted if not explicitly set.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » `google_storage_transfer_job`

Creates a new Transfer Job in Google Cloud Storage Transfer.

To get more information about Google Cloud Storage Transfer, see:

- Overview

- API documentation
- How-to Guides
  - Configuring Access to Data Sources and Sinks

## » Example Usage

Example creating a nightly Transfer Job from an AWS S3 Bucket to a GCS bucket.

```
data "google_storage_transfer_project_service_account" "default" {
  project = "${var.project}"
}

resource "google_storage_bucket" "s3-backup-bucket" {
  name          = "${var.aws_s3_bucket}"
  storage_class = "NEARLINE"
  project       = "${var.project}"
}

resource "google_storage_bucket_iam_member" "s3-backup-bucket" {
  bucket      = "${var.aws_s3_bucket}"
  role        = "roles/storage.admin"
  member      = "serviceAccount:${data.google_storage_transfer_project_service_account.default.service_account_email}"
  depends_on  = [
    "google_storage_bucket.s3-backup-bucket"
  ]
}

resource "google_storage_transfer_job" "s3-bucket-nightly-backup" {
  description = "Nightly backup of S3 bucket"
  project     = "${var.project}"

  transfer_spec {
    object_conditions {
      max_time_elapsed_since_last_modification = "600s"
      exclude_prefixes = [
        "requests.gz"
      ]
    }
    transfer_options {
      delete_objects_unique_in_sink = false
    }
    aws_s3_data_source {
      bucket_name = "${var.aws_s3_bucket}"
      aws_access_key {

```

```

        access_key_id      = "${var.aws_access_key}"
        secret_access_key   = "${var.aws_secret_key}"
    }
}
gcs_data_sink {
    bucket_name = "${var.aws_s3_bucket}-backup"
}
}

schedule {
    schedule_start_date {
        year      = 2018
        month      = 10
        day        = 1
    }
    schedule_end_date {
        year      = 2019
        month      = 1
        day        = 15
    }
    start_time_of_day {
        hours      = 23
        minutes     = 30
        seconds     = 0
        nanos       = 0
    }
}

depends_on = [
    "google_storage_bucket_iam_member.s3-backup-bucket"
]
}

```

## » Argument Reference

The following arguments are supported:

- **description** - (Required) Unique description to identify the Transfer Job.
- **transfer\_spec** - (Required) Transfer specification. Structure documented below.
- **schedule** - (Required) Schedule specification defining when the Transfer Job should be scheduled to start, end and and what time to run. Structure documented below.

- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
- **status** - (Optional) Status of the job. Default: `ENABLED`. **NOTE: The effect of the new job status takes place during a subsequent job run. For example, if you change the job status from `ENABLED` to `DISABLED`, and an operation spawned by the transfer is running, the status change would not affect the current operation.**

The `transfer_spec` block supports:

- **gcs\_data\_sink** - (Required) A Google Cloud Storage data sink. Structure documented below.
- **object\_conditions** - (Optional) Only objects that satisfy these object conditions are included in the set of data source and data sink objects. Object conditions based on objects' `last_modification_time` do not exclude objects in a data sink. Structure documented below.
- **transfer\_options** - (Optional) Characteristics of how to treat files from datasource and sink during job. If the option `delete_objects_unique_in_sink` is true, object conditions based on objects' `last_modification_time` are ignored and do not exclude objects in a data source or a data sink. Structure documented below.
- **gcs\_data\_source** - (Optional) A Google Cloud Storage data source. Structure documented below.
- **aws\_s3\_data\_source** - (Optional) An AWS S3 data source. Structure documented below.
- **http\_data\_source** - (Optional) An HTTP URL data source. Structure documented below.

The `schedule` block supports:

- **schedule\_start\_date** - (Required) The first day the recurring transfer is scheduled to run. If `schedule_start_date` is in the past, the transfer will run for the first time on the following day. Structure documented below.
- **schedule\_end\_date** - (Optional) The last day the recurring transfer will be run. If `schedule_end_date` is the same as `schedule_start_date`, the transfer will be executed only once. Structure documented below.
- **start\_time\_of\_day** - (Optional) The time in UTC at which the transfer will be scheduled to start in a day. Transfers may start later than this time. If not specified, recurring and one-time transfers that are scheduled to run today will run immediately; recurring transfers that are scheduled to run on a future date will start at approximately midnight UTC on that date. Note that when configuring a transfer with the Cloud Platform Console, the transfer's start time in a day is specified in your local timezone. Structure documented below.

The `object_conditions` block supports:

- `max_time_elapsed_since_last_modification` - (Optional) A duration in seconds with up to nine fractional digits, terminated by 's'. Example: "3.5s".
- `min_time_elapsed_since_last_modification` - (Optional) A duration in seconds with up to nine fractional digits, terminated by 's'. Example: "3.5s".
- `include_prefixes` - (Optional) If `include_refixes` is specified, objects that satisfy the object conditions must have names that start with one of the `include_prefixes` and that do not start with any of the `exclude_prefixes`. If `include_prefixes` is not specified, all objects except those that have names starting with one of the `exclude_prefixes` must satisfy the object conditions. See Requirements.
- `exclude_prefixes` - (Optional) `exclude_prefixes` must follow the requirements described for `include_prefixes`. See Requirements.

The `transfer_options` block supports:

- `overwrite_objects_already_existing_in_sink` - (Optional) Whether overwriting objects that already exist in the sink is allowed.
- `delete_objects_unique_in_sink` - (Optional) Whether objects that exist only in the sink should be deleted. Note that this option and `delete_objects_from_source_after_transfer` are mutually exclusive.
- `delete_objects_from_source_after_transfer` - (Optional) Whether objects should be deleted from the source after they are transferred to the sink. Note that this option and `delete_objects_unique_in_sink` are mutually exclusive.

The `gcs_data_sink` block supports:

- `bucket_name` - (Required) Google Cloud Storage bucket name.

The `gcs_data_source` block supports:

- `bucket_name` - (Required) Google Cloud Storage bucket name.

The `aws_s3_data_source` block supports:

- `bucket_name` - (Required) S3 Bucket name.
- `aws_access_key` - (Required) AWS credentials block.

The `aws_access_key` block supports:

- `access_key_id` - (Required) AWS Key ID.
- `secret_access_key` - (Required) AWS Secret Access Key.

The `http_data_source` block supports:

- **list\_url** - (Required) The URL that points to the file that stores the object list entries. This file must allow public access. Currently, only URLs with HTTP and HTTPS schemes are supported.

The **schedule\_start\_date** and **schedule\_end\_date** blocks support:

- **year** - (Required) Year of date. Must be from 1 to 9999.
- **month** - (Required) Month of year. Must be from 1 to 12.
- **day** - (Required) Day of month. Must be from 1 to 31 and valid for the year and month.

The **schedule\_start\_date** blocks support:

- **hours** - (Required) Hours of day in 24 hour format. Should be from 0 to 23
- **minutes** - (Required) Minutes of hour of day. Must be from 0 to 59.
- **seconds** - (Optional) Seconds of minutes of the time. Must normally be from 0 to 59.
- **nanos** - (Required) Fractions of seconds in nanoseconds. Must be from 0 to 999,999,999.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **name** - The name of the Transfer Job.
- **creation\_time** - When the Transfer Job was created.
- **last\_modification\_time** - When the Transfer Job was last modified.
- **deletion\_time** - When the Transfer Job was deleted.

## » Import

Storage buckets can be imported using the Transfer Job's **project** and **name** without the **transferJob/** prefix, e.g.

```
$ terraform import google_storage_transfer_job.nightly-backup-transfer-job my-project-1asd3
```



## » google\_kms\_crypto\_key

Allows creation of a Google Cloud Platform KMS CryptoKey. For more information see the official documentation and API.

A CryptoKey is an interface to key material which can be used to encrypt and decrypt data. A CryptoKey belongs to a Google Cloud KMS KeyRing.

Note: CryptoKeys cannot be deleted from Google Cloud Platform. Destroying a Terraform-managed CryptoKey will remove it from state and delete all CryptoKeyVersions, rendering the key unusable, but **will not delete the resource on the server**. When Terraform destroys these keys, any data previously encrypted with these keys will be irrecoverable. For this reason, it is strongly recommended that you add lifecycle hooks to the resource to prevent accidental destruction.

## » Example Usage

```
resource "google_kms_key_ring" "my_key_ring" {
  name     = "my-key-ring"
  project  = "my-project"
  location = "us-central1"
}

resource "google_kms_crypto_key" "my_crypto_key" {
  name           = "my-crypto-key"
  key_ring       = "${google_kms_key_ring.my_key_ring.self_link}"
  rotation_period = "100000s"

  lifecycle {
    prevent_destroy = true
  }
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) The CryptoKey's name. A CryptoKey's name must be unique within a location and match the regular expression `[a-zA-Z0-9_-]{1,63}`
- **key\_ring** - (Required) The id of the Google Cloud Platform KeyRing to which the key shall belong.

- **rotation\_period** - (Optional) Every time this period passes, generate a new `CryptoKeyVersion` and set it as the primary. The first rotation will take place after the specified period. The rotation period has the format of a decimal number with up to 9 fractional digits, followed by the letter `s` (seconds). It must be greater than a day (ie, 86400).
- **version\_template** - (Optional) A template describing settings for new crypto key versions. Structure is documented below.

---

The **version\_template** block supports:

- **algorithm** - (Required) The algorithm to use when creating a version based on this template. See the algorithm reference for possible inputs.
- **protection\_level** - (Optional) The protection level to use when creating a version based on this template. One of **SOFTWARE**, or **HSM**.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **self\_link** - The self link of the created `CryptoKey`. Its format is `projects/{projectId}/locations/{location}/keyRings/{keyRingName}/cryptoKeys/{cryptoKeyName}`.

## » Import

`CryptoKeys` can be imported using the `CryptoKey` autogenerated id, e.g.

```
$ terraform import google_kms_crypto_key.my_crypto_key my-gcp-project/us-central1/my-key-ring
```

```
$ terraform import google_kms_crypto_key.my_crypto_key us-central1/my-key-ring/my-crypto-key
```

## » google\_kms\_crypto\_key\_iam\_binding

Allows creation and management of a single binding within IAM policy for an existing Google Cloud KMS crypto key.

**Note:** On create, this resource will overwrite members of any existing roles. Use `terraform import` and inspect the `terraform plan` output to ensure your existing members are preserved.

## » Example Usage

```
resource "google_kms_crypto_key_iam_binding" "crypto_key" {
  crypto_key_id = "my-gcp-project/us-central1/my-key-ring/my-crypto-key"
  role          = "roles/editor"

  members = [
    "user:alice@gmail.com",
  ]
}
```

## » Argument Reference

The following arguments are supported:

- **members** - (Required) A list of users that the role should apply to. For more details on format and restrictions see <https://cloud.google.com/billing/reference/rest/v1/Policy#Binding>
- **role** - (Required) The role that should be applied. Only one `google_kms_crypto_key_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **crypto\_key\_id** - (Required) The crypto key ID, in the form `{project_id}/{location_name}/{key_ring_name}/{crypto_key_name}` or `{location_name}/{key_ring_name}/{crypto_key_name}`. In the second form, the provider's project setting will be used as a fallback.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the crypto key's IAM policy.

## » Import

IAM binding imports use space-delimited identifiers; first the resource in question and then the role. These bindings can be imported using the `crypto_key_id` and `role`, e.g.

```
$ terraform import google_kms_crypto_key_iam_binding.crypto_key "my-gcp-project/us-central1/
```

## » google\_kms\_crypto\_key\_iam\_member

Allows creation and management of a single member for a single binding within the IAM policy for an existing Google Cloud KMS crypto key.

**Note:** This resource *must not* be used in conjunction with `google_kms_crypto_key_iam_policy` or they will fight over what your policy should be. Similarly, roles controlled by `google_kms_crypto_key_iam_binding` should not be assigned to using `google_kms_crypto_key_iam_member`.

### » Example Usage

```
resource "google_kms_crypto_key_iam_member" "crypto_key" {
  crypto_key_id = "your-crypto-key-id"
  role          = "roles/editor"
  member        = "user:alice@gmail.com"
}
```

### » Argument Reference

The following arguments are supported:

- **member** - (Required) The user that the role should apply to. For more details on format and restrictions see <https://cloud.google.com/billing/reference/rest/v1/Policy#Binding>
- **role** - (Required) The role that should be applied. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **crypto\_key\_id** - (Required) The key ring ID, in the form `{project_id}/{location_name}/{key_ring_name}` or `{location_name}/{key_ring_name}/{crypto_key_name}`. In the second form, the provider's project setting will be used as a fallback.

### » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the project's IAM policy.

### » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the

crypto\_key\_id, role, and member identity e.g.

```
$ terraform import google_kms_crypto_key_iam_member.member "your-project-id/location-name/k
```

## » google\_\_kms\_\_key\_\_ring

Allows creation of a Google Cloud Platform KMS KeyRing. For more information see the official documentation and API.

A KeyRing is a grouping of CryptoKeys for organizational purposes. A KeyRing belongs to a Google Cloud Platform Project and resides in a specific location.

Note: KeyRings cannot be deleted from Google Cloud Platform. Destroying a Terraform-managed KeyRing will remove it from state but **will not delete the resource on the server**.

### » Example Usage

```
resource "google_kms_key_ring" "my_key_ring" {  
  name      = "my-key-ring"  
  location = "us-central1"  
}
```

### » Argument Reference

The following arguments are supported:

- **name** - (Required) The KeyRing's name. A KeyRing's name must be unique within a location and match the regular expression `[a-zA-Z0-9_-]{1,63}`
- **location** - (Required) The Google Cloud Platform location for the KeyRing. A full list of valid locations can be found by running `gcloud kms locations list`.

- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.

### » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- `self_link` - The self link of the created KeyRing. Its format is `projects/{projectId}/locations/{location}/keyRings/{keyRingName}`.

## » Import

KeyRings can be imported using the KeyRing autogenerated id, e.g.

```
$ terraform import google_kms_key_ring.my_key_ring my-gcp-project/us-central1/my-key-ring
```

```
$ terraform import google_kms_key_ring.my_key_ring us-central1/my-key-ring
```

## » IAM policy for Google Cloud KMS key ring

Three different resources help you manage your IAM policy for KMS key ring. Each of these resources serves a different use case:

- `google_kms_key_ring_iam_policy`: Authoritative. Sets the IAM policy for the key ring and replaces any existing policy already attached.
- `google_kms_key_ring_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the key ring are preserved.
- `google_kms_key_ring_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the key ring are preserved.

**Note:** `google_kms_key_ring_iam_policy` **cannot** be used in conjunction with `google_kms_key_ring_iam_binding` and `google_kms_key_ring_iam_member` or they will fight over what your policy should be.

**Note:** `google_kms_key_ring_iam_binding` resources **can be** used in conjunction with `google_kms_key_ring_iam_member` resources **only if** they do not grant privilege to the same role.

### » `google_kms_key_ring_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}
```

```
resource "google_kms_key_ring_iam_policy" "key_ring" {
  key_ring_id = "your-key-ring-id"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

#### » google\_kms\_key\_ring\_iam\_binding

```
resource "google_kms_key_ring_iam_binding" "key_ring" {
  key_ring_id = "your-key-ring-id"
  role        = "roles/editor"

  members = [
    "user:jane@example.com",
  ]
}
```

#### » google\_kms\_key\_ring\_iam\_member

```
resource "google_kms_key_ring_iam_member" "key_ring" {
  key_ring_id = "your-key-ring-id"
  role        = "roles/editor"
  member      = "user:jane@example.com"
}
```

### » Argument Reference

The following arguments are supported:

- **key\_ring\_id** - (Required) The key ring ID, in the form `{project_id}/{location_name}/{key_ring_name}` or `{location_name}/{key_ring_name}`. In the second form, the provider's project setting will be used as a fallback.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.

- **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
- **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_kms_key_ring_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_kms_key_ring_iam_policy`) The policy data generated by a `google_iam_policy` data source.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the key ring's IAM policy.

## » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the `key_ring_id`, role, and account e.g.

```
$ terraform import google_kms_key_ring_iam_member.key_ring_iam "your-project-id/location-name/key-ring-id/role/account"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role. This binding resource can be imported using the `key_ring_id` and role, e.g.

```
$ terraform import google_kms_key_ring_iam_binding.key_ring_iam "your-project-id/location-name/key-ring-id/role"
```

IAM policy imports use the identifier of the resource in question. This policy resource can be imported using the `key_ring_id`, role, and account e.g.

```
$ terraform import google_kms_key_ring_iam_policy.key_ring_iam "your-project-id/location-name/key-ring-id/role/account"
```

## » IAM policy for Google Cloud KMS key ring

Three different resources help you manage your IAM policy for KMS key ring. Each of these resources serves a different use case:

- **google\_kms\_key\_ring\_iam\_policy**: Authoritative. Sets the IAM policy for the key ring and replaces any existing policy already attached.



- `google_kms_key_ring_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the key ring are preserved.
- `google_kms_key_ring_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the key ring are preserved.

**Note:** `google_kms_key_ring_iam_policy` **cannot** be used in conjunction with `google_kms_key_ring_iam_binding` and `google_kms_key_ring_iam_member` or they will fight over what your policy should be.

**Note:** `google_kms_key_ring_iam_binding` resources **can be** used in conjunction with `google_kms_key_ring_iam_member` resources **only if** they do not grant privilege to the same role.

## » `google_kms_key_ring_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"

    members = [
      "user:jane@example.com",
    ]
  }
}

resource "google_kms_key_ring_iam_policy" "key_ring" {
  key_ring_id = "your-key-ring-id"
  policy_data = "${data.google_iam_policy.admin.policy_data}"
}
```

## » `google_kms_key_ring_iam_binding`

```
resource "google_kms_key_ring_iam_binding" "key_ring" {
  key_ring_id = "your-key-ring-id"
  role        = "roles/editor"

  members = [
    "user:jane@example.com",
  ]
}
```

## » google\_kms\_key\_ring\_iam\_member

```
resource "google_kms_key_ring_iam_member" "key_ring" {  
  key_ring_id = "your-key-ring-id"  
  role        = "roles/editor"  
  member      = "user:jane@example.com"  
}
```

## » Argument Reference

The following arguments are supported:

- **key\_ring\_id** - (Required) The key ring ID, in the form `{project_id}/{location_name}/{key_ring_name}` or `{location_name}/{key_ring_name}`. In the second form, the provider's project setting will be used as a fallback.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.
  - **user:{emailid}**: An email address that represents a specific Google account. For example, `alice@gmail.com` or `joe@example.com`.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`.
  - **group:{emailid}**: An email address that represents a Google group. For example, `admins@example.com`.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, `google.com` or `example.com`.
- **role** - (Required) The role that should be applied. Only one `google_kms_key_ring_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
- **policy\_data** - (Required only by `google_kms_key_ring_iam_policy`) The policy data generated by a `google_iam_policy` data source.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the key ring's IAM policy.

## » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the `key_ring_id`, role, and account e.g.

```
$ terraform import google_kms_key_ring_iam_member.key_ring_iam "your-project-id/location-name"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role. This binding resource can be imported using the `key_ring_id` and role, e.g.

```
$ terraform import google_kms_key_ring_iam_binding.key_ring_iam "your-project-id/location-name"
```

IAM policy imports use the identifier of the resource in question. This policy resource can be imported using the `key_ring_id`, role, and account e.g.

```
$ terraform import google_kms_key_ring_iam_policy.key_ring_iam your-project-id/location-name
```

## » IAM policy for Google Cloud KMS key ring

Three different resources help you manage your IAM policy for KMS key ring. Each of these resources serves a different use case:

- `google_kms_key_ring_iam_policy`: Authoritative. Sets the IAM policy for the key ring and replaces any existing policy already attached.
- `google_kms_key_ring_iam_binding`: Authoritative for a given role. Updates the IAM policy to grant a role to a list of members. Other roles within the IAM policy for the key ring are preserved.
- `google_kms_key_ring_iam_member`: Non-authoritative. Updates the IAM policy to grant a role to a new member. Other members for the role for the key ring are preserved.

**Note:** `google_kms_key_ring_iam_policy` **cannot** be used in conjunction with `google_kms_key_ring_iam_binding` and `google_kms_key_ring_iam_member` or they will fight over what your policy should be.

**Note:** `google_kms_key_ring_iam_binding` resources **can be** used in conjunction with `google_kms_key_ring_iam_member` resources **only if** they do not grant privilege to the same role.

## » `google_kms_key_ring_iam_policy`

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/editor"
```

```

        members = [
            "user:jane@example.com",
        ]
    }
}

resource "google_kms_key_ring_iam_policy" "key_ring" {
    key_ring_id = "your-key-ring-id"
    policy_data = "${data.google_iam_policy.admin.policy_data}"
}

```

## » google\_kms\_key\_ring\_iam\_binding

```

resource "google_kms_key_ring_iam_binding" "key_ring" {
    key_ring_id = "your-key-ring-id"
    role        = "roles/editor"

    members = [
        "user:jane@example.com",
    ]
}

```

## » google\_kms\_key\_ring\_iam\_member

```

resource "google_kms_key_ring_iam_member" "key_ring" {
    key_ring_id = "your-key-ring-id"
    role        = "roles/editor"
    member      = "user:jane@example.com"
}

```

## » Argument Reference

The following arguments are supported:

- **key\_ring\_id** - (Required) The key ring ID, in the form `{project_id}/{location_name}/{key_ring_name}` or `{location_name}/{key_ring_name}`. In the second form, the provider's project setting will be used as a fallback.
- **member/members** - (Required) Identities that will be granted the privilege in **role**. Each entry can have one of the following values:
  - **allUsers**: A special identifier that represents anyone who is on the internet; with or without a Google account.
  - **allAuthenticatedUsers**: A special identifier that represents anyone who is authenticated with a Google account or a service account.

- **user:{emailid}**: An email address that represents a specific Google account. For example, alice@gmail.com or joe@example.com.
  - **serviceAccount:{emailid}**: An email address that represents a service account. For example, my-other-app@appspot.gserviceaccount.com.
  - **group:{emailid}**: An email address that represents a Google group. For example, admins@example.com.
  - **domain:{domain}**: A G Suite domain (primary, instead of alias) name that represents all the users of that domain. For example, google.com or example.com.
- **role** - (Required) The role that should be applied. Only one `google_kms_key_ring_iam_binding` can be used per role. Note that custom roles must be of the format `[projects|organizations]/{parent-name}/roles/{role-name}`.
  - **policy\_data** - (Required only by `google_kms_key_ring_iam_policy`) The policy data generated by a `google_iam_policy` data source.

## » Attributes Reference

In addition to the arguments listed above, the following computed attributes are exported:

- **etag** - (Computed) The etag of the key ring's IAM policy.

## » Import

IAM member imports use space-delimited identifiers; the resource in question, the role, and the account. This member resource can be imported using the `key_ring_id`, role, and account e.g.

```
$ terraform import google_kms_key_ring_iam_member.key_ring_iam "your-project-id/location-name"
```

IAM binding imports use space-delimited identifiers; the resource in question and the role. This binding resource can be imported using the `key_ring_id` and role, e.g.

```
$ terraform import google_kms_key_ring_iam_binding.key_ring_iam "your-project-id/location-name"
```

IAM policy imports use the identifier of the resource in question. This policy resource can be imported using the `key_ring_id`, role, and account e.g.

```
$ terraform import google_kms_key_ring_iam_policy.key_ring_iam your-project-id/location-name"
```

## » google\_\_cloudiot\_\_registry

Creates a device registry in Google's Cloud IoT Core platform. For more information see the official documentation and API.

### » Example Usage

```
resource "google_pubsub_topic" "default-devicestatus" {
  name = "default-devicestatus"
}

resource "google_pubsub_topic" "default-telemetry" {
  name = "default-telemetry"
}

resource "google_cloudiot_registry" "default-registry" {
  name = "default-registry"

  event_notification_config = {
    pubsub_topic_name = "${google_pubsub_topic.default-telemetry.id}"
  }

  state_notification_config = {
    pubsub_topic_name = "${google_pubsub_topic.default-devicestatus.id}"
  }

  http_config = {
    http_enabled_state = "HTTP_ENABLED"
  }

  mqtt_config = {
    mqtt_enabled_state = "MQTT_ENABLED"
  }

  credentials = [
    {
      public_key_certificate = {
        format      = "X509_CERTIFICATE_PEM"
        certificate = "${file("rsa_cert.pem")}"
      }
    },
  ]
}
```

## » Argument Reference

The following arguments are supported:

- **name** - (Required) A unique name for the resource, required by device registry. Changing this forces a new resource to be created.
- 
- **project** - (Optional) The project in which the resource belongs. If it is not provided, the provider project is used.
  - **region** - (Optional) The Region in which the created address should reside. If it is not provided, the provider region is used.
  - **event\_notification\_config** - (Optional) A PubSub topics to publish device events. Structure is documented below.
  - **state\_notification\_config** - (Optional) A PubSub topic to publish device state updates. Structure is documented below.
  - **mqtt\_config** - (Optional) Activate or deactivate MQTT. Structure is documented below.
  - **http\_config** - (Optional) Activate or deactivate HTTP. Structure is documented below.
  - **credentials** - (Optional) List of public key certificates to authenticate devices. Structure is documented below.

The **event\_notification\_config** block supports:

- **pubsub\_topic\_name** - (Required) PubSub topic name to publish device events.

The **state\_notification\_config** block supports:

- **pubsub\_topic\_name** - (Required) PubSub topic name to publish device state updates.

The **mqtt\_config** block supports:

- **mqtt\_enabled\_state** - (Required) The field allows **MQTT\_ENABLED** or **MQTT\_DISABLED**.

The **http\_config** block supports:

- **http\_enabled\_state** - (Required) The field allows **HTTP\_ENABLED** or **HTTP\_DISABLED**.

The **credentials** block supports:

- **public\_key\_certificate** - (Required) The certificate format and data.

The **public\_key\_certificate** block supports:

- `format` - (Required) The field allows only `X509_CERTIFICATE_PEM`.
- `certificate` - (Required) The certificate data.

## » Attributes Reference

Only the arguments listed above are exposed as attributes.

## » Import

A device registry can be imported using the `name`, e.g.

```
$ terraform import google_cloudiot_registry.default-registry projects/{project}/locations/{location}/registries/{registry-name}
```