Network tags are text attributes you can add to Compute Engine (/compute/docs/) virtual machine (VM) instances. Tags allow you to make firewall rules (/vpc/docs/firewalls) and routes (/vpc/docs/routes) applicable to specific VM instances.

You can only add network tags to VM instances or instance templates (/compute/docs/instance-templates/). You cannot tag other Google Cloud resources. You can assign network tags to new instances at creation time, or you can edit the set of assigned tags at any time later. Network tags can be edited without stopping an instance.

The network tags that you assign to an instance only apply to the VPC network (/vpc/docs/vpc) where the instance's primary network interface is located. This is true even for VPC Network Peering (/vpc/docs/vpc-peering), because peered networks remain distinct networks. Thus, the network tags are still only meaningful in the network that contains the instance's primary network interface.

Network tags must start with a lowercase letter and can contain lowercase letters, numbers, and hyphens. Tags must end with a lowercase letter or number.

Networks tags don't need to be unique across multiple VPC networks. The same tags can be used in different networ
purposes in each.

The following IAM roles are required for tasks discussed on this page. For more details, see Compute Engine IAM roles (/compute/docs/access/iam).

Task	Required Role
Assign a network tag to a new instance when it is created	Project owner or editor (/iam/docs/understanding-roles#primitive_roles) *or* Instance Admin (/compute/docs/access/iam#compute.instanceAdmin.v1)
Add or remove network tags for existing instances	
Add, remove, or edit firewall rules	Project owner or editor (/iam/docs/understanding-roles#primitive_roles) *or*

	Security Admin (/compute/docs/access/iam#compute.securityAdmin)

The following limits apply to network tags:

Limit	Value	Description
Maximum number of tags per VM	64	All tags for a VM must be unique. You can assign up to 64 different tags per VM.
Maximum number of characters for each tag	63	
Acceptable characters for a tag	lowercase letters, numbers, dashes	Additionally: • Tags must start with a lowercase letter. • Tags must end with either a number or a lowercase letter.

Network tags allow you to apply firewall rules and routes to a specific instance or set of instances:

- You make a firewall rule applicable to specific instances by using target tags and source tags.
- You make a route applicable to specific instances by using a tag.

Every firewall rule in Google Cloud must have a target (/vpc/docs/firewalls#rule_assignment) which defines the instances to which it applies. The default target is *all instances in the network*, but you can specify instances as targets using either target tags or target service accounts.

The *target tag* defines the Google Cloud VMs to which the rule applies. The rule will be made applicable to the primary internal IP address of any instance having a matching network tag.

Both ingress and egress firewall rules have targets:

- Ingress rules apply to traffic entering your VPC network. For ingress rules, the targets are *destination* VMs in Google Cloud.

- Egress rules apply to traffic leaving your VPC network. For egress rules, the targets are *source* VMs in Google Cloud.

Consider an ingress firewall rule that allows traffic on TCP port `80` from any source. The rule has a target tag of `http-server`. This rule would apply only to instances that have the `http-server` network tag, which means that incoming traffic on port `80` would be allowed to those instances.

When you create *ingress* firewall rules, you must specify a source (/vpc/docs/firewalls#sources_or_destinations_for_the_rule). You can define it using ranges of either internal or external IP addresses or by referring to specific instances. You specify instances using either source tags or source service accounts.

The *source tag* for an ingress firewall rule defines a source of traffic as coming from the primary internal IP address of any instance having a matching network tag.

You can use a combination of IP ranges and source tags or a combination of IP ranges and source service accounts (/compute/docs/access/service-accounts). You **cannot** use both network tags and service accounts in the same rule. For more information about source tags and service accounts, see filtering by service account vs. network tag (/vpc/docs/firewalls#service-accounts-vs-tags).

When you use an ingress firewall rule with source tags, you might observe a propagation delay. This delay is typically a few seconds, but it can be, in rare cases, a few minutes. When you make the following changes, the ingress firewall rule can take time to apply to or be removed from an associated instance:

- Starting or stopping an instance that has a tag that is associated with a rule's source tag
- Starting an instance that has a tag that is associated with a rule's target tag
- Adding or removing tags from an instance if the tags are used in the source or target fields of a rule
- Adding or removing source or target tags from a rule

This propagation delay applies only to ingress rules that use source tags. All other firewall rules take effect immediately on an instance. For example, an ingress rule that uses a source IP address range and target tags has no propagation delay.

When you create a route, you can specify *tags* so that it is only applicable to traffic sent from the primary internal IP address of instances with matching network tags.

You can set the network tags associated with an instance by making a direct API request. Unlike using the Cloud Console or `gcloud` commands, updating tags by direct API request **does not preserve** any existing tags. Ensure that you specify **the complete set** of tags that should be associated with an instance whenever you update tags in this way.

To update tags using a direct API request:

1. Determine the latest fingerprint associated with the tags. The fingerprint is used to prevent any collisions from simultaneous API requests. The process of updating network tags for an instance is similar to updating instance metadata (/compute/docs/metadata#update_metadata_on_a_running_instance).

   Perform a `GET` request to the instance; for example:

   Look for the `tags.fingerprint` property in the response:

   You can also use a `gcloud` command to get the `fingerprint`, as shown in the following example:

2. Make a `POST` request to the `instance().setTags` method. The request body must contain **all** of the tags that should be associated with the instance along with the `fingerprint` value.

   Example request:

   Example response:

- See Firewall Rules Overview (/vpc/docs/firewalls) and Using Firewall Rules (/vpc/docs/using-firewalls) for more about how to work with firewall rules in Google Cloud.
- See Routes Overview (/vpc/docs/routes) and Using Routes (/vpc/docs/using-routes) for more about how to work with routes in Google Cloud.