



# Configure High Availability in Cisco Catalyst 8000V Running On Google Cloud Platform

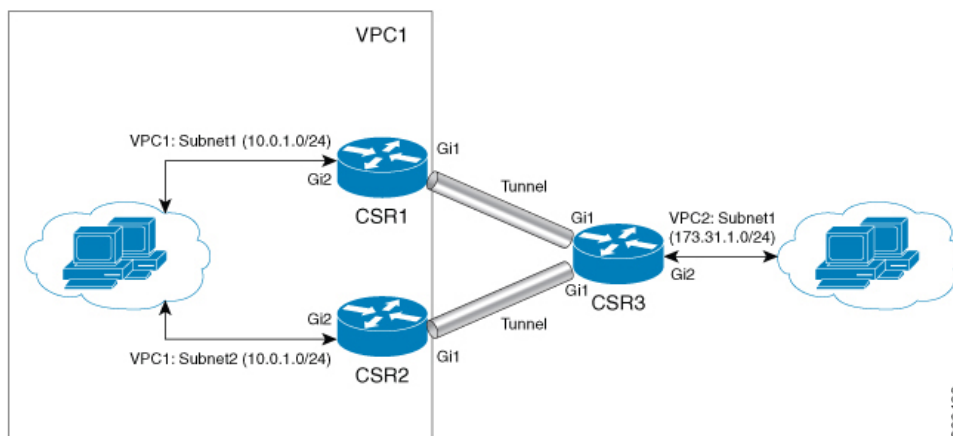
---

In the Google cloud, each static route belongs to the route table associated with a VPC and consists of following fields:

- **Name and Description:** These fields identify the route. A name is required, but a description is optional. Every route in your project must have a unique name.
- **Network:** Each route must be associated with exactly one VPC network.
- **Destination range:** The destination range is a single IPv4 CIDR block containing the IP addresses of systems that receive incoming packets. GCP does not support IPv6 destination ranges. Destinations must be expressed in CIDR notation, and the broadest destination possible is 0.0.0.0/0.
- **Priority:** Priority is used to determine which route should be used if multiple routes have identical destinations. Lower numbers indicate higher priorities; for example, a route with a priority value of 100 has a higher priority than one with a priority value of 200.
- **Next hop:** Static routes can have next hops that point to the default Internet gateway, a GCP instance, or a Cloud VPN tunnel. Refer to static route next hops for more information.
- **Tags:** You can specify a list of network tags so that the route will only apply to instances that have at least one of the listed tags. If you don't specify tags, GCP applies the route to all instances in the network.

For more information, see <https://cloud.google.com/vpc/docs/routes>. To configure High Availability in an active/active operation for two Cisco Catalyst 8000V routers in the Google network, you must create two routes in the route collection for each destination range, where each route points to one of the two routers as the next hop.

To understand this better, consider the following topology:



In the above topology, there are two routers configured in the HA mode. Both the routers have one interface in VPC1 and another in VPC. These two Cisco Catalyst 8000V routers have a Tunnel configured to another Cisco Catalyst 8000V instance that has an interface in VPC2. In this scenario, the following are the route entries in VPC1 for destination range of VPC 2 (172.31.0.0/16):

route-vcp2-c8000v1	172.31.0.0/16	100	None	IP:10:1:0:3	test-vpc
route-vcp2-c8000v2	172.31.0.0/16	200	None	IP:10:0:2:3	test-vpc

The active route is decided based on the route priority. Since route-vcp2-c8000v1 has a lower value, this route has a higher priority, thereby making Cisco Catalyst 8000V 1 as the active route.

### Reversion to Primary Cisco Catalyst 8000V After Fault Recovery

If Cisco Catalyst 8000V 1 fails, Cisco Catalyst 8000V 2 detects a peer fail event through the BFD tunnel and deletes route-vcp2-c8000v1 from route collection making route-vcp2-c8000v2 as the active route for destination range 172.31.0.0/16.

When Cisco Catalyst 8000V 1 recovers, it adds route-vcp2-c8000v1 route back to the route collection which makes it the primary route again for all traffic to VPC 2. Please note it is possible to set equal route priority for both route entries in which case Google cloud uses both routes to send traffic to destination range.

On each Cisco Catalyst 8000V instance, you must create nodes corresponding to each route entry in route collection with next hop as the two Cisco Catalyst 8000V instances.

When you use the mode (primary or secondary) option in HA to create a new node, ensure that the route with the higher priority (lower number) is marked as primary and the route with lower priority is marked as secondary.

### User-Supplied Scripts

The guestshell is a container in which you can deploy your own scripts. High Availability exposes a programming interface to user-supplied scripts, so you can write scripts that can trigger both failover and reversion events. You can develop your own algorithms and triggers to control which Cisco Catalyst 8000V provides the forwarding services for a given route.

- [Cloud Specific Configuration of Redundancy Parameters, on page 3](#)
- [Create a Redundancy Node, on page 4](#)
- [Set Redundancy Node Parameters, on page 5](#)

- [Authenticate the Cisco Catalyst 8000V Router, on page 5](#)

## Cloud Specific Configuration of Redundancy Parameters

Parameter	Is this parameter required?	Switch	Description
Node Index	Yes	-i	The index that is used to uniquely identify this node. Valid values: 1–255.
Cloud Provider	Yes	-p	Specify gcp for this parameter.
Project	Yes	-g	Specify the Google Project ID.
routeName	Yes	-a	The route name for which this Cisco Catalyst 8000V is next hop. For example from Fig. 2, if we are configuring node on Cisco Catalyst 8000V 1, this would be route-vpc2-c8000v1.
peerRouteName	Yes	-b	The route name for which the BFD peer Cisco Catalyst 8000V is next hop. For example from Fig. 2, if we are configuring node on Cisco Catalyst 8000V 1, this would be route-vpc2-c8000v2.
Route	yes	-r	<p>The IP address of the route to be updated in CIDR format. Can be IPv4 or IPv6 address.</p> <p>If a route is unspecified, then the redundancy node is considered to apply to all routes in the routing table of type virtual appliance.</p> <p>Note: Currently Google cloud does not have IPv6 support in VPC.</p>

Parameter	Is this parameter required?	Switch	Description
Next hop address	Yes	-n	The IP address of the next hop router. Use the IP address that is assigned to this Cisco Catalyst 8000V on the subnet which utilizes this route table. The value can be an IPv4 or IPv6 address.  Note: Currently Google cloud does not have IPv6 support in VPC.
hopPriority	Yes	-o	The route priority for the route for which the current Cisco Catalyst 8000V is the next hop.
VPC	Yes	-v	The VPC network name where the route with the current Cisco Catalyst 8000V as the next hop exists.

## Create a Redundancy Node

### Procedure

Run the following script to create a redundancy node and add it to the database: `create_node { switch value } [...[{ switch value }]]`.

You must configure the following parameters for a valid redundancy node:

- Node Index
- Cloud Provider
- Project ID
- Route Name
- Peer Route Name
- Route
- Next Hop Address
- Hop Priority

- VPC Name

```
create_node -i 1 -g <project-id> -r dest_network -o 200 -n nexthop_ip_addr -a route-name1 -b route-name2  
-p gcp -v vpc_name
```

If the configuration is successful, the script returns a value of zero.

---

## Set Redundancy Node Parameters

### Procedure

---

To change the value of parameters in an existing redundancy node, run the following script: `set_params{ switch value } [...[{ switch value }]]`.

#### Example:

```
set_params -i 10 -r 15.0.0.0/16 -n 172.168.7.5
```

The index parameter (-i) is mandatory. This command sets the values of the specified parameters. If the specified parameter is already defined for the redundancy node, the value of the parameter is updated.

When a node index value of zero is specified, the values that are provided by the command for the specified parameters are treated as the default values for these parameters.

If this configuration is successful, the script returns a value of zero.

---

## Authenticate the Cisco Catalyst 8000V Router

### SUMMARY STEPS

1. Ensure that the service account associated with the Cisco Catalyst 8000V routers at least have a Compute Network Admin permission.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Ensure that the service account associated with the Cisco Catalyst 8000V routers at least have a Compute Network Admin permission.	<div>Create service account</div> <div><div>1 Service account details</div><div>2 Grant this service account access to project (optional)</div><div>3 Grant users access to this project</div></div> <div><div>Service account permissions (optional)</div><div>Grant this service account access to project-avvyas so that it has permission to complete specific actions on the resources in your project. <a href="#">Learn more</a></div><div><div>Select a role</div><div>Type to filter</div><div><div>Cloud TPU</div><div>Cloud Trace</div><div>Codelab API Keys</div><div>Compute Engine</div><div>Container Analysis</div><div>Custom</div><div>Dataflow</div></div><div><div>Compute Admin</div><div>Compute Image User</div><div>Compute Instance Admin (beta)</div><div>Compute Instance Admin (v1)</div><div>Compute Load Balancer Admin</div><div>Compute Network Admin</div><div>Compute Network User</div><div>Compute Network Viewer</div></div><div>MANAGE ROLES</div></div><div><div>Compute Network Admin</div><div>Full control of Compute Engine networking resources.</div></div></div> <div>You can also provide the required permissions in a credentials file with name 'credentials.json' and place it under the /home/guestshell directory. The credentials file overrides the permissions supplied through the service account associated with the Cisco Catalyst 8000V instance.</div>