Table of Contents

1. Introduction ................................................................................................................. 3
3. Accessing GCP ............................................................................................................. 4
4. GCP Management ........................................................................................................ 4 Accessing the GCP Portal ...................................................................................................... 4 GCP CLI & GCP API ............................................................................................................... 4
5. Deploying Enterprise GCP from the Marketplace ......................................................... 4 To Reserve a static private IP address for the appliance ................................................... 8 To Reserve A static public IP address for the appliance ..................................................... 9
6. Accessing the Appliance ............................................................................................... 10 Accessing the Appliance using the WebUI ......................................................................... 10 WebUI Menu Options .......................................................................................................... 11 Appliance Security ............................................................................................................... 11 Security Mode ....................................................................................................................... 11 Passwords ............................................................................................................................ 12 Security Lockdown Script ..................................................................................................... 12 Checking For Updates ........................................................................................................ 13 Appliance Licensing ............................................................................................................. 13 Accessing the Appliance using SSH .................................................................................. 13 Generating SSH Keys ........................................................................................................... 13 Update the GCP project metadata ....................................................................................... 15 Accessing the Appliance from Linux ................................................................................ 16 Accessing the Appliance from Windows using PuTTY ....................................................... 16 Accessing the Appliance with the GCP User Credentials .................................................. 17
8. Testing – General Comments ....................................................................................... 32 Testing Load Balanced Services ........................................................................................... 33 Diagnosing VIP Connection Problems ............................................................................ 33 Taking Real Servers Offline .............................................................................................. 34 Using Reports & Log Files ................................................................................................ 35
10. Loadbalancer.org Technical Support ........................................................................... 35
1. Introduction

Google Cloud Platform (GCP) is a broad suite of cloud-based services running on the same global infrastructure as Googles popular end-user products, such as Search and YouTube. It allows services to be deployed as and when required. Charges are made for what is used making it an extremely flexible and cost-effective solution. It offers scalable services deployed from a variety of management tools, such as WebUI and API. The Loadbalancer.org Enterprise GCP cloud based load balancer allows customers to rapidly deploy and configure a feature rich load balancing solution within the GCP cloud environment.

2. About Enterprise GCP

The core software is based on customized versions of Centos 6.x/RHEL 6.x, Linux 4.9.x, LVS, HA-Linux, HAProxy, Pound, STunnel & Ldirectord. At present, Enterprise GCP is available as a single appliance only due to the nature of the network design/constraints. HA (high-availability) clustering may be available in the future. Enterprise GCP is based on the same code base as our main hardware/virtual product. This means that Enterprise GCP supports many of the same features as the hardware & virtual based products. There are certain differences due to the way the GCP environment works. The main differences are listed below.

**Note**

Currently, Enterprise GCP can have one network interface. This interface has a single primary internal IP address. A single external public IP can be associated with the primary IP to expose load balanced services on the public Internet. Additional load balanced services can be presented on the same IP address using different ports.

Multiple services on different internal IP addresses can be configured using Alias IPs. For a deployment example please refer to Example 2 – Web Servers: Single Subnet, Layer 7, Internal Facing.

If you want to present additional services on different External IPs, a GCP load balancers (either HTTP(S), TCP or UDP) can be used to terminate additional public IP addresses. For more information and a deployment example, please refer to Example 4 – using GCP Load balancer To Present Multiple Services on Different Public IPs.

**Main Differences to Our Standard (Non-Cloud) Product**

1. Layer 4 DR mode is currently not supported.

2. HA (high availability) where a clustered pair of appliances is deployed is currently not supported.

3. Layer 4 NAT mode where the default gateway on the load balanced real servers is set to be the load balancer is not supported.

   - Instead, add a tagged route that only applies to traffic from the load balanced servers and set the next hop to be the load balancer – please refer to Example 3 – Web Servers: Single Subnet, Layer 4, Public Facing for an example of how VPC routing is modified to route traffic back via the load balancer.

4. Layer 7 SNAT mode with TProxy enabled where the default gateway on the load balanced real servers is required to be the load balancer is not supported.

   - Instead, add a tagged route that only applies to traffic from the load balanced servers and set the next hop to be the load balancer – please refer to Example 3 – Web Servers: Single Subnet, Layer 4, Public Facing for an example of how VPC routing is modified to route traffic back via the load balancer.

5. Enterprise GCP can have only one network interface.
Why use Enterprise GCP?

Google’s load balancer provides basic load balancing functionality but is limited in several areas. Loadbalancer.org’s Enterprise GCP load balancer provides the following additional features & advantages:

1. Supports comprehensive Layer 7 load balancing.
2. Load balances both GCP based and non-GCP based servers.
4. Supports customizable timeouts for custom applications beyond those offered by GCP.
5. Supports comprehensive back-end server health-check options.
6. Enables fallback servers to be configured and invoked when all load balanced servers/services fail.
7. Provides extensive real time and historical statistics reports.
8. Supports session distribution based on actual server load (utilizing Loadbalancer.org’s feedback agent which is available for both Linux & Windows).
9. Supports SSL Termination.
10. Supports Microsoft RDP Cookie based persistence.

3. Accessing GCP

To start using GCP, you will need a Google account. If you don’t already have one you can create one at the following URL: https://cloud.google.com/

4. GCP Management

GCP resources can be managed in various ways:

- GCP Portal
- Gcloud CLI
- GCP API

Accessing the GCP Portal

The GCP Portal can be access here.

GCP CLI & GCP API

- Information on how to obtain, install and configure Gcloud CLI is available here.
- Information on how to obtain, install and configure GCP API is available here.

5. Deploying Enterprise GCP from the Marketplace

1. Login into the GCP Portal.
2. Select Marketplace from the menu and search for "Loadbalancer.org", you’ll be presented with the following three options:
   - Loadbalancer.org Enterprise GCP R20 – hourly billing with up to 5 VIPs / 4 RIPs
- **Loadbalancer.org Enterprise GCP MAX** – hourly billing with unlimited VIPs / RIPS
- **Loadbalancer.org Enterprise GCP BYOL** – for purchasing & applying your own license

**Note**

The BYOL version will work completely unrestricted for 30 days without any license applied. During this period, only Google Compute usage charges will apply. After the 30 days, the trial will still function, but no configuration changes will be possible until the license is applied.

3. Click on the option you require, you will be presented with a more detailed overview of the product.
4. Click the **Launch** button.

---

**New Loadbalancer.org Enterprise GCP BYOL deployment**

<table>
<thead>
<tr>
<th>Deployment name</th>
<th>lb1</th>
</tr>
</thead>
</table>

**Zone**

- Europe-West2-C

**Machine type**

**Machine family**

- **GENERAL-PURPOSE**
- **COMPUTE-OPTIMISED**
- **MEMORY-OPTIMISED**

Machine types for common workloads, optimised for cost and flexibility

<table>
<thead>
<tr>
<th>Series</th>
<th>N1</th>
</tr>
</thead>
</table>

Powered by Intel Skylake CPU platform or one of its predecessors

<table>
<thead>
<tr>
<th>Machine type</th>
<th>n1-standard-1 (1 vCPU, 3.75 GB memory)</th>
</tr>
</thead>
</table>

**CPU PLATFORM AND GPU**

- Enter an appropriate **Deployment Name**
- Select the required **Zone**
- Configure the **Machine Type** settings according to your requirements

5. Scroll down to the **Boot disk & Networking** sections.
Configure the Boot disk type according to your requirements, these options can normally be left at their default values.

Configure the Network Interfaces settings according to your requirements.

**Note:** The internal IP and the external IP of the load balancer instance can be promoted to static addresses rather than ephemeral after deployment. This is described further below.

Scroll down to the Firewall section.
The following firewall rules are automatically configured for each VPC network:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Targets</th>
<th>Filters</th>
<th>Protocol/ports</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>test-allow-icmp</td>
<td>Ingress</td>
<td>Apply to all</td>
<td>IP ranges: 0.0.0.0/0</td>
<td>icmp</td>
<td>Allow</td>
</tr>
<tr>
<td>test-allow-internal</td>
<td>Ingress</td>
<td>Apply to all</td>
<td>IP ranges: 10.128.0.0/9</td>
<td>all</td>
<td>Allow</td>
</tr>
<tr>
<td>test-allow-rdp</td>
<td>Ingress</td>
<td>Apply to all</td>
<td>IP ranges: 0.0.0.0/0</td>
<td>tcp:3389</td>
<td>Allow</td>
</tr>
<tr>
<td>test-allow-ssh</td>
<td>Ingress</td>
<td>Apply to all</td>
<td>IP ranges: 0.0.0.0/0</td>
<td>tcp:22</td>
<td>Allow</td>
</tr>
</tbody>
</table>

When the Loadbalancer.org appliance is deployed, a new firewall rule is automatically added to enable access to the WebUI on port 9443. This is controlled by the option *Allow TCP port 9443 traffic from the Internet* shown above.

Filters should be configured where possible to limit access to specific source IP ranges.

If you plan to use Layer 4 NAT or Layer 7 with TProxy ensure that *IP Forwarding* is **On**.

Add additional rules as required by your deployment.

For layer 7 deployments, you'll need to allow access on TCP port 7777 to enable access to the Layer 7 Stats page.

**Note**

When troubleshooting connection issues, you can disable a firewall rule rather than deleting it. Select the rule, select **EDIT** and navigate to the *Enforcement* section, select **Disabled** and click **SAVE**.

6. Click **Deploy** – a deployment summary page will be displayed:
The auto generated temporary password that is used to login as the WebUI user 'loadbalancer' should be changed once you login.

If the instance has an external IP, you can directly access the WebUI after deployment by clicking the Visit the Site button.

If you have deployed a BYOL appliance, you automatically have a 30 day trial. The Request a License link takes you to the loadbalancer.org website to purchase a license.

An ephemeral external IP is assigned to the appliance. For production deployments this should be changed to a static address.

**Warning**

Do **NOT** change the private IP of the appliance using the appliance’s WebUI. This will not update the GCP network stack and make the appliance completely unusable. There is currently no recovery from this and you’ll need to deploy a new instance.

To Reserve a static private IP address for the appliance

1. Using the GCP console, edit the instance.
2. In the Network Interfaces section change Internal IP type to **Static**.
3. In the popup, specify an appropriate Name & Description.

4. Click Reserve.

5. Scroll to the end of the page and click Save.

To Reserve A static public IP address for the appliance

1. Using the GCP console, edit the instance.

2. In the Network Interfaces section change External IP type to Create IP address.

3. In the popup, specify an appropriate Name & Description.

4. Set the Network Service Tier according to your requirements.

5. Click Reserve.

6. Scroll to the end of the page and click Save.
6. Accessing the Appliance

Accessing the Appliance using the WebUI

As mentioned above, you can access the appliance immediately from the deployment screen by clicking the Visit the Site button. This will open a new browser window and connect to https://<instance-public-ip>:9443. Alternatively, open a browser and navigate to the Public IP address on port 9443, i.e.

https://<Public IP Address>:9443
or
https://<FQDN>:9443

Note: Google Cloud VPC networks have an internal DNS service and do not automatically support configuring external DNS for a VM.

You'll receive a warning about the certificate as it's a self signed cert not related to an Internet based CA. Confirm you want to continue and a login prompt will be displayed. Use the following default credentials:

Username: loadbalancer
Password: <temporary-password>

The temporary-password is displayed in the deployment summary page after deployment and also in the custom metadata section of the VM instance properties in the GCP console:

<table>
<thead>
<tr>
<th>Custom metadata</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>loadbalancer_user_password</td>
<td>X7f0eKYB0uN8</td>
</tr>
<tr>
<td>google-monitoring-enable</td>
<td>0</td>
</tr>
<tr>
<td>google-logging-enable</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: To change the password for the 'loadbalancer' account, use the WebUI option: Maintenance > Passwords. Changing the password in the appliance will not update the temporary password displayed in the GCP overview.

Once logged in, the WebUI is displayed:
WebUI Menu Options

System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
Local Configuration - Configure local host settings such as IP address, DNS, system time etc.
Cluster Configuration - Configure load balanced services such as VIPs & RIPs
Maintenance - Perform maintenance tasks such as service restarts and taking backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links
Live Chat - Start a Live Chat session with one of our Support Engineers

Appliance Security

Security Mode
To control how the appliance is accessed and which features are enabled, 3 security modes are provided:

- Secure - this is the default mode. In this mode:
  - the WebUI is accessible on HTTPS port 9443. If you attempt to access the WebUI on HTTP port 9080 you will be redirected to HTTPS port 9443
- access to the Local Configuration > Execute shell command menu option is disabled
- the ability to edit the firewall script & the lockdown wizard is disabled
- 'root' user console & SSH password access are disabled
- **Custom** - In this mode, the security options can be configured to suit your requirements
- **Secure - Permanent** - this mode is the same as Secure but the change is **irreversible**

**Important** | Only set the security mode to **Secure - Permanent** if you are 100% sure this is what you want!

*To configure the Security Mode:*

1. Using the WebUI, navigate to: Local Configuration > Security.
2. Select the required Appliance Security Mode.
3. If Custom is selected, configure the additional options according to your requirements.
4. Click Update.

**Note** | For more information on configuring appliance security, please refer to Appliance Security Options.

**Passwords**

The password for the 'loadbalancer' WebUI user account and the 'root' Linux user account are set during the Network Setup Wizard. These can also be changed at any time as explained below:

1 - the 'root' Linux account:

As explained above, 'root' user console & SSH password access are disabled by default. If enabled, the 'root' password should be changed at the console, or via an SSH session using the following command:

```
# passwd
```

**Note** | For the AWS and Azure cloud products it’s not possible to directly login as root. If root access is required, once you’ve logged into the console/SSH session using the credentials defined during instance deployment, run the following command:

```
$ sudo su
```

2 - the 'loadbalancer' WebUI account:

This can be changed using the WebUI menu option: Maintenance > Passwords.

**Security Lockdown Script**

The appliance also includes a security lockdown command (lbsecure) that enables passwords to be set, network access to be locked down and SSH key regeneration in one simple step. This command can be run on a single appliance or an HA pair. For more information please refer to Appliance Security Lockdown Script.
Checking For Updates

Once you have access to the WebUI, we recommend that you use the online update feature to ensure that you’re running the very latest version of the appliance. To check for updates, use the WebUI option: Maintenance > Software Update and click the Online Update button. If updates are available, you’ll be presented with a list of changes that are included in the update. To start the update, click the second Online Update button at the bottom of the screen. Updates are incremental, so repeat the process until you’re informed that no more updates are available.

Appliance Licensing

If you’ve deployed the BYOL version of the appliance, by default it runs as a 30 day trial and is completely unrestricted during this time. After 30 days, the appliance continues to work but it’s no longer possible to make changes to the configuration. When a license is purchased, you’ll be provided with a license key file by our sales team. This must then be installed on your appliance. To install the license, use the WebUI option: Local Configuration > License Key to browse to and select the license file provided. Once selected, click Install License Key to apply the license. We recommend that you should check for updates before applying the license key.

Accessing the Appliance using SSH

When the appliance is deployed, the projects users and SSH keys are inherited from GCP Compute Engine Metadata, making secure access easier to manage. To SSH into the appliance, you will need to ensure that the public SSH key file in the Compute Engines Metadata is correct and that the matching private SSH key file is on the device you are using.

More information on managing SSH keys in GCP can be found here.

To access the appliance via SSH, either via Windows or Linux, it is recommended to use a client application rather than from the GCP browser.

Generating SSH Keys

The steps below show how to generate SSH key pairs using Linux and Windows, before copying the public key to GCP Project Metadata. If you already have keys setup in GCP you can skip this step.

Using Linux

STEP 1 - Generate a keypair using ssh-keygen

All Distros:

```
# ssh-keygen -q -t rsa -b 2048 -f <output filename>
```

e.g.

```
# ssh-keygen -q -t rsa -b 2048 -f GCPKeys
```

When prompted, enter a pass-phrase, or leave empty for no passphrase:

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```
2 files are created:

- **GCPKeys** – this is the Private Key file and is used on the SSH client machine
- **GCPKeys.pub** – this is the Public Key file, the contents are copied into the *SSH public key* field when the VM is deployed.

Using Windows

**STEP 1 – Install PuTTY**

1. Download PuTTY from [here](#).
2. Run the installer.

**STEP 2 – Use PuTTYgen to generate a Public/Private key pair**

1. Browse to the PuTTY program folder and run PuTTYgen.

2. Click the **Generate** button.
3. As directed, move the mouse around to create random keys.
4. Once generated, enter **root** in the **Key comment** field as shown above and then copy the public key from the top window / save it to a file.

**Update the GCP project metadata**

If you are an existing user in the relevant GCP Project then you should be able to SSH into the appliance. However, if you have generated new SSH keys or are adding a new client device, you will need to update the GCP Project Metadata keys.

1. Access the GCP portal and navigate to **Compute Engine > Metadata > SSH Keys** and click the **Edit** button.

2. Click **Add Item** and paste the contents of the public key file (e.g GCPKeys.pub or the data displayed at the top in PuTTYgen) into the window, as shown in the following example:

3. Click **Save** – the updated public key will be added to the metadata for that project.
Accessing the Appliance from Linux
Start SSH specifying the private key file and login as the "root" user, e.g.:

Using the IP address:

```
# ssh -i GCPKeys root@1.2.3.4
```

Accessing the Appliance from Windows using PuTTY

1. Run PuTTY.
2. Expand the SSH section and select Auth as shown below:

3. Click **Browse** and select the private key created earlier.
4. Click **Open** to start the SSH session.
5. Login using root and the password you have specified (default is loadbalancer).
It’s highly recommend to change the default root password and regenerate the ssh keys after deployment of the appliance.

To change the root password at the command line:

```bash
passwd root
```

To regenerate the ssh keys at the command line:

```bash
lbsecure ssh
```

Accessing the Appliance with the GCP User Credentials

It is possible to log into the appliance via SSH with the GCP user credentials, if the users public key is correctly recognized in the Compute Engine Metadata, as described previously.

If using the GCP user credentials via SSH, some commands may need root credentials to run, and can be executed using "sudo" to achieve elevated privileges.

7. Deployment examples

The following section provides 3 examples to help illustrate how the load balancer can be deployed. It is important to consider that when configured at layer 7, the load balancer acts as a proxy and is not transparent which means that the source IP address of packets reaching the real servers will be the load balancer’s own IP address.

Example 1 – Web Servers: Single Subnet, Layer 7, Public facing

This is a simple layer 7 example using one subnet for both the load balancer and the web servers.

a) Deploying the GCP instances

1. Deploy the load balancer instance as described in the section Deploying Enterprise GCP from the Marketplace, configure a static External IP address – this must be done after deployment.

2. Deploy your web server instances into the same VPC & subnet as the load balancer, use a static Internal IP address – this can either be reserved in advance and assigned during deployment or promoted after deployment.

3. Ensure that firewall rules allow external access to the load balancer on HTTP port 80.

b) Setting up the Virtual Service

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Services and click Add a New Virtual Service.

2. Enter the following details:
3. Enter an appropriate label for the VIP, e.g. WebCluster1.

4. Set the Virtual Service IP address field to the Base IP address, e.g. 10.154.0.17.

5. Set the Virtual Service Ports field to the required port, e.g. 80.


7. Click Update.

c) Setting up the Real Servers

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created VIP.

2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>Web1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.154.0.18</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>80</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label for the RIP, e.g. Web1.

4. Set the Real Server IP Address field to the required IP address, e.g. 10.154.0.18.

5. Set the Real Server Port field to the required port, e.g. 80.

6. Click Update.

7. Repeat the above steps to add your other web server(s).

d) Applying the new Layer 7 Settings

1. Once the configuration is complete, use the Reload HAProy button at the top of the screen to apply the
changes.

e) Testing

1. Connect to the external IP address of the load balancer instance on port 80 to verify that the web page is displayed.

Example 2 – Web Servers: Single Subnet, Layer 7, Internal Facing

This example shows how a VIP can be configured on an IP Alias. This allows multiple internal/private VIPs to be configured on different IP addresses.

a) Deploying the GCP Instances

1. Deploy the load balancer instance as described in the section Deploying Enterprise GCP from the Marketplace, configure a static Internal IP address – this must be done after deployment.

2. Deploy your web server instances into the same VPC & subnet as the load balancer, use a static Internal IP address – this can either be reserved in advance and assigned during deployment or promoted after deployment.

3. Ensure that firewall rules allow internal access to the load balancer on HTTP port 80.

b) Configuring the Alias IP

1. Using the GCP console, edit the load balancer instance.

2. Scroll down to the Network Interfaces section and click the edit button.

3. Click Show alias IP ranges.

4. Enter the required Alias IP – this will be used for the new VIP (the /32 will be added automatically).

5. Click Done, click Save.

c) Setting up the Virtual Service

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Services and click Add a New Virtual Service.

2. Enter the following details:
3. Enter an appropriate label for the VIP, e.g. **WebCluster2**.

4. Set the Virtual Service IP address field to the **Alias IP address**, e.g. **10.154.0.50**.

5. Set the Virtual Service Ports field to the required port, e.g. **80**.

6. Leave Layer 7 Protocol set to **HTTP Mode**.

7. Click **Update**.

d) Setting up the Real Servers

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Real Servers** and click **Add a new Real Server** next to the newly created VIP.

2. Enter the following details:

   - **Label**: **Web1**
   - **Real Server IP Address**: **10.154.0.18**
   - **Real Server Port**: **80**
   - Leave **Re-Encrypt to Backend** unchecked.
   - **Weight**: **100**

3. Enter an appropriate label for the RIP, e.g. **Web1**.

4. Set the Real Server IP Address field to the required IP address, e.g. **10.154.0.18**.

5. Set the Real Server Port field to the required port, e.g. **80**.

6. Click **Update**.

7. Repeat the above steps to add your other web server(s).

e) Applying the new Layer 7 Settings

1. Once the configuration is complete, use the **Reload HAProxy** button at the top of the screen to apply the changes.
f) Testing

1. Connect to the IP Alias address of the load balancer instance on port 80 to verify that the web page is displayed.

Example 3 – Web Servers: Single Subnet, Layer 4, Public Facing

This is a layer 4 (NAT mode) example using one subnet for both the load balancer and the web servers. In this example, VPC routing must be configured to route return traffic from the web servers via the load balancer. This is achieved by adding a route for all destination IP ranges (0.0.0.0/0), setting the next hop as the load balancer and using tags to ensure this route only applies to the load balanced web servers.

a) Deploying the GCP Instances

1. Deploy the load balancer instance as described in the section Deploying Enterprise GCP from the Marketplace, configure a static External IP address – this must be done after deployment.

2. Deploy your web server instances into the same VPC & subnet as the load balancer, use a static Internal IP address – this can either be reserved in advance and assigned during deployment or promoted after deployment.

3. Ensure that firewall rules allow external access to the load balancer on HTTP port 80.

b) Configuring GCP Routing

1. Using the GCP console, select Routes in the VPC menu.

2. Click CREATE ROUTE.
3. Enter an appropriate Name, e.g. route-via-lb.
4. Select the relevant Network, e.g. default.
5. Set the Destination Ip Range to 0.0.0.0/0.
6. Set the priority higher (lower number) than the default 0.0.0.0/0 route, e.g. 900.
7. Enter an instance tag to filter which instances the rule applies to, e.g. route-via-lb.
8. Set Next Hop to Specify an instance.
9. Set the Next hop instance to the load balancer.
10. Click CREATE.

c) Tagging the Web Server instances

1. Using the GCP console, Edit each web server instance.
2. In the Network Tags section add a tag with the same name as used for the route tag above, e.g. route-via-lb.
3. Click Save.

d) Setting up the Virtual Service

1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Virtual Services and click Add a New Virtual Service.
2. Enter the following details:

<table>
<thead>
<tr>
<th>Virtual Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Forwarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding Method</td>
</tr>
</tbody>
</table>

3. Enter an appropriate Label for the VIP, e.g. WebCluster1.

4. Set the IP address to the Base IP address, e.g. 10.154.0.17.

5. Set the Ports to the required port, e.g. 80.

6. Set Protocol to TCP.

7. Set Forwarding Method to NAT.

8. Click Update.

e) Setting up the Real Servers

1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Real Servers and click Add a new Real Server next to the newly created VIP.

2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Real Server IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.154.0.18</td>
</tr>
</tbody>
</table>

| Real Server Port      | 80          |
|-----------------------|
| Weight                | 100         |

| Minimum Connections   | 0           |
|-----------------------|
| Maximum Connections   | 0           |

3. Enter an appropriate label for the RIP, e.g. Web1.

4. Set the Real Server IP Address to the required IP value, e.g. 10.154.0.18.

5. Set the Real Server Port to the required port, e.g. 80.
6. Click **Update**.

7. Repeat the above steps to add your other web server(s).

**f) Testing**

1. Connect to the external IP address of the load balancer instance on port 80 to verify that the web page is displayed.

**Example 4 – using GCP Load balancer To Present Multiple Services on Different Public IPs**

This example shows how a GCP load balancer can be used to present multiple services on different public IP addresses. The first service can be presented in the load balancer’s public IP address, other services are presented via the GCP load balancer. In this case there is no need to configure a health-check on the GCP load balancer, traffic will always be forwarded to the Loadbalancer.org appliance.

The following 3 services will be configured:

- **Service 1** – Web Cluster 1 presented on public IP 1 (the External IP of the instance)
- **Service 2** – Web Cluster 2 presented on public IP 2 (additional External IP reserved for service 2)
- **Service 3** – Custom application 1 presented on public IP 3, TCP/UDP port 2050 (additional External IP reserved for service 3)

**a) Deploying the GCP Instances**

1. Deploy the load balancer instance as described in the section [Deploying Enterprise GCP from the Marketplace](#), configure a static External IP address – this must be done after deployment.

2. Deploy your web server instances and custom application instances to the same VPC & subnet as the load balancer, use a static Internal IP address – this can either be reserved in advance and assigned during deployment or promoted after deployment.

3. Ensure that firewall rules allow external access to the load balancer on HTTP port 80.

**b) Configure Service 1**

1. Configure service 1 using [Example 1 – Web Servers: Single Subnet, Layer 7, Public facing](#) as a guide, Service 1 will then be presented on the Loadbalancer.org appliance’s public IP address.

**c) Add a GCP Load Balancer & Configure Service 2**

1. Navigate in the GCP Console to Network Services > Load balancing and click Create Load balancer.

2. Under TCP Load Balancing click Start Configuration.
3. Leave the defaults and click Continue.

4. Type a Name for the load balancer, e.g. gcplb1.

5. Click Backend Configuration.

   - **Name**: gcplb1
   - **Region**: europe-west2
   - **Backends**: Select existing instance groups
     - **lb100-vm (europe-west2-c)**
     - **Add an instance**

   - **Backup pool**: None

   - **Failover ratio**: 10%

   - **Health check**: No health check

   - **Session affinity**: None

6. Set the Region according to your requirements.
7. Under **Backends** click **Select existing instances**.

8. In the **Add an instance** drop-down, select the Loadbalancer.org load balancer instance.

9. Leave the remaining settings at their default values.

10. Click **Frontend Configuration** and then click **Add Frontend IP and port**.

![New Frontend IP and port](image)

11. Enter a suitable **Name**, e.g. *service2*.

12. Under **IP**, select **Create IP address**.

13. Enter an appropriate **Name**, e.g. *service2*.

14. Click **Reserve**.

15. Specify the required **Port**, e.g. *80*.

16. Click **Done**.

17. Click **Review and Finalize** – there will be a warning concerning no health checks but that can be ignored as we want all traffic to be sent to the Loadbalancer.org appliance.

18. Click **Create**.

d) **Configure Service 3 (TCP)**

1. Under the load balancing menu, click **advanced menu**.

2. Click **CREATE FORWARDING RULE**.
3. Enter a suitable Name, e.g. service3-tcp.
4. Select the appropriate Region.
5. Under External IP, select Create IP address.
6. Enter an appropriate Name, e.g. service3.
7. Click Reserve.
8. Set the Protocol to TCP.
9. Specify the required Port, e.g. 2050.
10. Under Target pool select the GCP load balancer just created, e.g gcplb1.
11. Click Create.

e) Configure Service 3 (UDP)

1. Click CREATE FORWARDING RULE.
2. Enter a suitable Name, e.g. service3-udp.
3. Select the appropriate Region.
5. Set the Protocol to UDP.
6. Specify the required Port, e.g. 2050.

7. Under Target pool select the GCP load balancer just created, e.g gcplb1.

8. Click Create.

f) Verify forwarding Rules

The following forwarding rules will be displayed:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Region</th>
<th>Address</th>
<th>Protocol</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>service2</td>
<td></td>
<td>Regional</td>
<td>europe-west2</td>
<td>34.89.33.219.88-80</td>
<td>tcp</td>
<td>gcplb1</td>
</tr>
<tr>
<td>service3-tcp</td>
<td></td>
<td>Regional</td>
<td>europe-west2</td>
<td>34.89.121.70.2050-2050</td>
<td>tcp</td>
<td>gcplb1</td>
</tr>
<tr>
<td>service3-udp</td>
<td></td>
<td>Regional</td>
<td>europe-west2</td>
<td>34.89.121.70.2050-2050</td>
<td>udp</td>
<td>gcplb1</td>
</tr>
</tbody>
</table>

+ 


g) Configure Routing to ensure return traffic for service3 routes back from the application servers via the loadbalancer.org instance as required by Layer 4 NAT mode


h) Configure VIPs on the Loadbalancer.org appliance

1. Connect to the Loadbalancer.org appliance WebUI.

Configure Service 1

1. Navigate to Cluster Configuration > Layer 7 Virtual Services and click Add a New Virtual Service.

   ![Virtual Service Form]

2. Enter an appropriate label, e.g. Service1.

3. Enter the appliance’s Internal IP address, e.g. 10.154.0.17.

4. Set the Ports field to 80.

5. Leave Layer 7 Protocol set to HTTP Mode.

6. Click Update.
7. Navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click *Add a new Real Server* next to the newly created VIP.

```
<table>
<thead>
<tr>
<th>Label</th>
<th>Web1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.154.0.18</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>80</td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td>No</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>
```

8. Enter an appropriate *label*, e.g. *Web1*.

9. Set the *Real Server IP Address* field to the required IP address, e.g. *10.154.0.18*.

10. Set the *Real Server port* field to *80*.

11. Click *Update*.

12. Repeat the above steps to add your other real server(s).

**Configure Service 2**

1. Navigate to *Cluster Configuration > Layer 7 Virtual Services* and click *Add a New Virtual Service*.

```
<table>
<thead>
<tr>
<th>Virtual Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Configuration</td>
</tr>
<tr>
<td>Label</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Ports</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
</tbody>
</table>
```

2. Enter an appropriate *label*, e.g. *Service2*.

3. Enter the External IP that was reserved for Service2 in the GCP console, e.g. *34.89.33.219*.

4. Set the *Ports* field to *80*.

5. Leave *Layer 7 Protocol* set to *HTTP Mode*.

6. Click *Update*.

7. Navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click *Add a new Real Server* next to the newly created VIP.
8. Enter an appropriate label, e.g. Web1.

9. Set the Real Server IP Address field to the required IP address, e.g. 10.154.0.19.

10. Set the Real Server port field to 80.

11. Click Update.

12. Repeat the above steps to add your other real server(s).

Configure Service 3 – TCP

1. Navigate to Cluster Configuration > Layer 4 Virtual Services and click Add a New Virtual Service

2. Enter an appropriate label, e.g. Service3-tcp.

3. Enter the External IP that was reserved for Service2 in the GCP console, e.g. 34.89.121.70.

4. Set the Ports field to 2050.

5. Set the Protocol to TCP.

6. Set the Forwarding Method to NAT.

7. Click Update.

8. Navigate to: Cluster Configuration > Layer 4 – Real Servers and click Add a new *Real Server next to the newly created VIP.
9. Enter an appropriate *label*, e.g. `app1`.

10. Set the *Real Server IP Address* field to the required IP address, e.g. `10.154.0.20`.

11. Set the *Real Server port* field to `80`.

12. Click **Update**.

13. Repeat the above steps to add your other real server(s).

Configure Service 3 – UDP

1. Navigate to `Cluster Configuration > Layer 4 Virtual Services` and click **Add a New Virtual Service**.

2. Enter an appropriate *label*, e.g. `Service3`.

3. Enter the External IP that was reserved for Service2 in the GCP console, e.g. `34.89.121.70`.

4. Set the *Ports* field to `2050`.

5. Set the *Protocol* to **UDP**.

6. Set the *Forwarding Method* to **NAT**.

7. Click **Update**.

8. Navigate to: `Cluster Configuration > Layer 4 – Real Servers` and click **Add a new Real Server** next to the newly created VIP.
9. Enter an appropriate label. e.g. \texttt{app1}.

10. Set the \textit{Real Server IP Address} field to the required IP address, e.g. \texttt{10.154.0.20}.

11. Set the \textit{Real Server port} field to \texttt{80}.

12. Click \texttt{Update}.

13. Repeat the above steps to add your other real server(s).

i) Verify VIPs

The VIPs will be displayed in the \textit{System Overview} of the WebUI:

![System Overview](image)

j) Testing

1. Verify that \texttt{service1:80} is available on the external IP of the Loadbalancer.org appliance.

2. Verify that \texttt{service2:80} is available on the IP address reserved for service 2.

3. Verify that \texttt{service3:2050 (TCP & UDP)} is available on the IP address reserved for service 3.

8. Testing – General Comments

\textbf{Note} For more information on testing and verifying load balanced services, please refer to \texttt{Testing Load Balanced Services} in the Administration Manual.
Testing Load Balanced Services

For example, to test a web server based configuration, add a page to each web servers root directory e.g. test.html and put the server name on this page for easy identification during the tests.

Use two or more clients to do the testing. Open up a web browser on each test clients and enter the URL for the VIP e.g. http://104.40.133.119

Provided that persistence is disabled, each client should see a different server name because of the load balancing algorithm in use, i.e. they are being load balanced across the cluster.

Why test using two clients? - If you use a single client it will most likely keep on hitting the same server for multiple requests. This is to do with the way that the load balancing algorithms are optimized.

Diagnosing VIP Connection Problems

1. Make sure that the device is active – this can be checked in the WebUI. For a single appliance, the status bar should report Primary & Active as shown below:

   ![Status Bar Screenshot]

2. Check that the VIP(s)/floating IP(s) are up – Using View Configuration > Network Configuration verify that the VIP is active on the load balancer, if not check Logs > Heartbeat for errors.

   ```
   2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
       link/ether 00:0c:29:cf:18:03 brd ff:ff:ff:ff:ff:ff
       inet 192.168.110.85/18 brd 192.168.127.255 scope global eth0
           valid_lft forever preferred_lft forever
       inet 192.168.110.90/18 brd 192.168.127.255 scope global secondary eth0
           valid_lft forever preferred_lft forever
   ```

   The above example shows that the interface address (192.168.110.85) and the VIP address (192.168.110.90) are both up.

3. Check that the Real Servers are up – Using System Overview make sure that none of your VIPs are colored red. If they are, the entire cluster is down (i.e. all Real Servers). Green indicates a healthy cluster, yellow indicates that your cluster may need attention (one or more of the Real Servers may be down), and blue indicates all Real Server have been deliberately taken offline (by using either Halt or Drain).
4. **Check the connection state:**

- **For layer 4 NAT mode VIPs**, check **Reports > Layer 4 Current Connections** to view the current traffic in detail. Any packets with state **SYN_RECV** often implies a return traffic routing issue:
  - For single subnet Layer 4 mode make sure that the default gateway on all real servers is set to be the load balancer
  - For dual subnet Layer 4 mode make sure that routing on the second subnet has been configured correctly
- **For Layer 7 VIPs**, the Layer 7 statistics page can be used. To access the page, navigate to: **Reports > Layer 7 Status** - a new tabbed window will be displayed:

### Statistics Report for pid 3261

#### General process information

<table>
<thead>
<tr>
<th>PID</th>
<th>State</th>
<th>Process Activity</th>
<th>Memory Use</th>
<th>Network Use</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>pid 3261 (process #1, pid=3261)</td>
<td>active UP</td>
<td>active UP</td>
<td>21888</td>
<td>32580</td>
<td>OPEN</td>
</tr>
</tbody>
</table>

- **Display option:**
  - **Show DOWN servers**
  - **Refresh now**
  - **Query options**
  - **Query results**

### Taking Real Servers Offline

1. Using the **System Overview** check that when you Halt one of the Real Servers the connections are redirected to the other server in the cluster.

2. Stop the web service/process on one of the servers, wait a few seconds (for the load balancer to detect the change) and then refresh the browsers on both clients. They should now both switch to the same server (since one has been removed from the load balancing list). Also check that the server is shown red (down) in the system overview.

3. Start the web service/process on the server, wait a few seconds and then refresh the browsers again. After a few refreshes they should again show different web servers. Also check that the server is shown green (up) in the system overview.

The **System Overview** shows the status as these tests are performed:

### System Overview

<table>
<thead>
<tr>
<th>HTTP-Cluster</th>
<th>IP</th>
<th>PORTS</th>
<th>CONNS</th>
<th>PROTOCOL</th>
<th>METHOD</th>
<th>MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.10.150</td>
<td>80</td>
<td>0</td>
<td>HTTP</td>
<td>Layer 7</td>
<td>Proxy</td>
<td></td>
</tr>
</tbody>
</table>

- **Real Server:**
  - **IP:**
    - RIPv: 192.168.1.10.240
    - RIPv2: 192.168.1.10.241
    - RIPv3: 192.168.1.10.242
  - **Weight:**
    - 100
  - **Connections:**
    - 0
  - **Status:**
    - Drain: Halt
  - **Mode:**
    - Online (Halt)
In this example:

**RIP1** is green, this indicates that it’s operating normally.

**RIP2** is blue, this indicates that it has been either Halted or Drained. in this example Halt has been used as indicated by Online (Halt) being displayed. If it had been drained it would show as Online (Drain).

**RIP3** is red, this indicates that it has failed a health check.

**Using Reports & Log Files**
The appliance includes several logs and reports that are very useful when diagnosing issues. Both are available as main menu options in the WebUI. Details of both can be found in *Appliance Monitoring*.

9. More Information

Please refer to our website for all the latest *Manuals* and *Deployment Guides*.

10. Loadbalancer.org Technical Support

If you have any questions regarding the appliance or need assistance with load balancing your application, please don’t hesitate to contact our support team using the following email address: support@loadbalancer.org.
About Loadbalancer.org
Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.