# Table of Contents

1. About this Brief .................................................. 3
2. Loadbalancer.org Appliances Supported ...................... 3
3. Software Versions Supported .................................... 3
   3.1. Loadbalancer.org Appliance ................................ 3
   3.2. Quantum ActiveScale ....................................... 3
4. Quantum ActiveScale ............................................ 3
5. Load Balancing Quantum ActiveScale .......................... 3
   5.1. Health Checks .................................................. 3
6. Load Balancer Deployment Methods ............................. 4
   6.1. 'Direct to Node' GSLB ....................................... 4
7. Loadbalancer.org Appliance – the Basics ...................... 5
   7.1. Virtual Appliance ............................................. 5
   7.2. Initial Network Configuration ............................... 5
   7.3. Accessing the Appliance WebUI ............................. 5
      Main Menu Options ........................................... 7
   7.4. Appliance Software Update .................................. 7
      Determining the Current Software Version ................. 7
      Checking for Updates using Online Update ................ 7
      Using Offline Update ......................................... 8
   7.5. Ports Used by the Appliance ............................... 8
   7.6. HA Clustered Pair Configuration ........................... 9
8. Appliance Configuration for Quantum ActiveScale ........... 9
   8.1. Overview ....................................................... 9
   8.2. Health Checks ................................................ 10
   8.3. Appliance Configuration ..................................... 11
      Step 1 – Configuring the Global Name ....................... 11
      Step 2 – Configure the Members ............................. 11
      Step 3 – Configure the Pool .................................. 12
      Step 4 – Finalising the Configuration ....................... 13
   8.4. DNS Server Configuration .................................. 13
   8.5. Testing the Configuration .................................. 13
9. Testing & Verification ........................................... 14
10. Technical Support ............................................... 14
11. Further Documentation ......................................... 14
12. Appendix ......................................................... 15
   12.1. Microsoft DNS Server Configuration ..................... 15
      Microsoft DNS Server ....................................... 15
   12.2. Configuring HA - Adding a Secondary Appliance ....... 17
      Non-Replicated Settings ..................................... 17
      Adding a Secondary Appliance - Create an HA Clustered Pair 18
13. Document Revision History ..................................... 21
1. About this Brief

This brief outlines the steps required to configure a load balanced Quantum ActiveScale environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Quantum ActiveScale configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with Quantum ActiveScale. For full specifications of available models please refer to https://www.loadbalancer.org/products.

Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.6.1 and later

Note: The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If using an older software version, note that the screenshots presented here may not match the WebUI exactly.

3.2. Quantum ActiveScale

- All versions

4. Quantum ActiveScale

Quantum ActiveScale is an object storage solution which provides a new and innovative approach to creating a simple, ‘always-on’ data repository that scales when needed. This is done with the extreme data durability, accessibility, and security required of petabyte-scale growth. As part of this solution, ActiveScale Cold Storage reduces the cost of storing cold data sets by up to 80%.

5. Load Balancing Quantum ActiveScale

Note: It’s highly recommended that you have a working Quantum ActiveScale environment first before implementing the load balancer.

5.1. Health Checks

GSLB-based health checks on port 443 are used to establish the health of the ActiveScale nodes.
6. Load Balancer Deployment Methods

For Quantum ActiveScale, using the somewhat uncommon “direct to node’ GSLB” deployment method is recommended. This mode is described below and is used for the configurations presented in this guide. For configuring using GSLB direct to node please refer to Section 8, “Appliance Configuration for Quantum ActiveScale”.

6.1. 'Direct to Node' GSLB

- Round-robin DNS with health checking
- Client traffic flows directly to the ActiveScale Nodes and directly back again – the load balancer is entirely removed from the path of ActiveStore traffic
- Useful when network throughput is paramount while retaining the load balancer’s active health checking of ActiveStore nodes

The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to the section Configuring HA - Adding a Secondary Appliance in the appendix for more details on configuring a clustered pair.

A full explanation and instructions on setting up this type of deployment can be found in Section 8, “Appliance Configuration for Quantum ActiveScale”.

© Copyright Loadbalancer.org • Documentation • Load Balancing Quantum ActiveScale
7. LoadBalancer.org Appliance – the Basics

7.1. Virtual Appliance

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.

![Image](https://example.com)

The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance’s WebUI.

![Image](https://example.com)

Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

![Image](https://example.com)

The VA has 4 network adapters. For VMware only the first adapter (eth0) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

7.2. Initial Network Configuration

After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS Server and other network settings.

![Image](https://example.com)

Be sure to set a secure password for the load balancer, when prompted during the setup routine.

7.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

![Image](https://example.com)

There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

![Image](https://example.com)

A number of compatibility issues have been found with various versions of Microsoft Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

1. Using a browser, navigate to the following URL:


![Image](https://example.com)

You’ll receive a warning about the WebUI’s certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more
2. Log in to the WebUI using the following credentials:

**Username**: loadbalancer  
**Password**: <configured-during-network-setup-wizard>

Note: To change the password, use the WebUI menu option: *Maintenance > Passwords*.

Once logged in, the WebUI will be displayed as shown below:

3. You’ll be asked if you want to run the Setup Wizard. Click **Dismiss** if you’re following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.
Main Menu Options

System Overview - Displays a graphical summary of all VIPs, RIPv 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 & RIPv
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

7.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

The software version is displayed at the bottom of the WebUI as shown in the example below:

Checking for Updates using Online Update

1. Using the WebUI, navigate to: Maintenance > Software Update.
2. Select Online Update.
3. If the latest version is already installed, a message similar to the following will be displayed:

   Information: Version v8.9.0 is the current release. No updates are available

4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click Online Update to start the update process.
6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

**Information: Update completed successfully.**

7. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

**Using Offline Update**

If the load balancer does not have access to the Internet, offline update can be used.

**Note**

Please contact support@loadbalancer.org to check if an update is available and obtain the latest offline update files.

**To perform an offline update:**

1. Using the WebUI, navigate to: **Maintenance > Software Update**.
2. Select **Offline Update**.
3. The following screen will be displayed:

**Software Update**

**Offline Update**

The following steps will lead you through offline update.

1. Contact loadbalancer.org support to obtain the offline update archive and checksum.
2. Save the archive and checksum to your local machine.
3. Select the archive and checksum files in the upload form below.
4. Click **Upload and Install** to begin the update process.

![Image of Software Update interface](image)

4. Select the **Archive** and **Checksum** files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

**7.5. Ports Used by the Appliance**

By default, the appliance uses the following TCP & UDP ports:
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>53</td>
<td>DNS</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>123</td>
<td>NTP</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>161</td>
<td>SNMP</td>
</tr>
<tr>
<td>UDP</td>
<td>6694</td>
<td>Heartbeat between Primary &amp; Secondary appliances in HA mode</td>
</tr>
<tr>
<td>TCP</td>
<td>7778</td>
<td>HAProxy persistence table replication</td>
</tr>
<tr>
<td>TCP</td>
<td>9080</td>
<td>WebUI - HTTP (disabled by default)</td>
</tr>
<tr>
<td>TCP</td>
<td>9081</td>
<td>Nginx fallback page</td>
</tr>
<tr>
<td>TCP</td>
<td>9443</td>
<td>WebUI - HTTPS</td>
</tr>
</tbody>
</table>

7.6. HA Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in the section Configuring HA - Adding a Secondary Appliance of the appendix.

8. Appliance Configuration for Quantum ActiveScale

8.1. Overview

In the context of a ‘GSLB only’, 'direct to node' configuration, the function of the load balancer is to ensure that connections to a Quantum ActiveScale cluster are distributed across the ActiveScale nodes. This is done to provide a highly available and scalable service. This is achieved by configuring the load balancers to actively health check the ActiveScale nodes and serve up the IP address of a healthy node in response to a (delegated) DNS request for the ActiveScale service’s domain.

Deployment Example:
**Explanation:**

- **Start:** A client tries to access the S3 service by using the service's fully qualified domain name, in this example `s3-region1.domain.tld`

- The client sends a DNS query for `s3-region1.domain.tld` to the DNS server.

- The DNS server has a CNAME record for `s3-region1.domain.tld` which points to the domain `gslb.domain.tld`

- The DNS server has the domain `gslb.domain.tld` delegated to the load balancers.

- The DNS server sends a delegated DNS query for `gslb.domain.tld` to one of the load balancers.

- The load balancer that received the delegated DNS query replies to the DNS server. The load balancer answers with the IP address of a healthy, online ActiveScale node. In this example, `10.0.0.11` is the IP address returned by the load balancer.

- The DNS server sends the delegated DNS answer to the client.

- **Finish:** The client connects to the S3 service at `s3-region1.domain.tld` by using the IP address of the ActiveScale node that it was served.

### 8.2. Health Checks

The GSLB service, when configured as described in this section, polls each Quantum ActiveScale node at a regular interval to determine its health. This is achieved by checking that TCP port 443 is open.
8.3. Appliance Configuration

The GSLB service should be configured on the primary load balancer appliance.

Configuration takes place in the WebUI under Cluster Configuration > GSLB Configuration:

Step 1 – Configuring the Global Name
1. Using the WebUI on the primary appliance, navigate to Cluster Configuration > GSLB Configuration.
2. Select the Global Names tab.
3. Click the New Global Name button.
4. Define a friendly Name for the new hostname, which can just be the subdomain itself, e.g. quantum.example.com
5. Define the Hostname of what will be the delegated subdomain, e.g. quantum.example.com
6. Click Submit.

Step 2 – Configure the Members
Each member is a single ActiveScale node.

1. Select the Members tab.
2. Click the New Member button.
3. Enter a friendly Name for the member, e.g. quantum-node1.
4. Specify an IP address for the member: in this context, this should be the IP address of the ActiveScale node in question, e.g. 10.0.0.11.

5. Ignore the example value in the Monitor IP field.

6. Click Submit.

7. Repeat these steps to add additional ActiveStore nodes as members as required.

---

**Step 3 – Configure the Pool**

A pool must be created to link together a global name with the members that should serve traffic for that global name.

Continuing with the example presented in this section, a pool would be created linking the global name quantum.example.com with the members (ActiveScale nodes), all of which should serve ActiveScale traffic.

1. Select the Pools tab.

2. Click the New Pool button.

3. Enter a friendly Name for the pool, e.g. quantum-nodes.

4. Set the Monitor to TCP.

5. Set Monitor Port to 443.

6. Set LB Method to wrr.

7. From the Global Names list box, select the global name in question, e.g. quantum.example.com

8. In the Members section, drag the appropriate members (ActiveStore nodes) from the Available Members box into the Members In Use box.

9. Click Submit.
Step 4 – Finalising the Configuration
To apply the new settings, the GSLB service must be restarted as follows:

1. Using the WebUI, navigate to: Maintenance > Restart Services and click Restart GSLB.

8.4. DNS Server Configuration
Once the GSLB service has been configured on the primary load balancer the DNS server must then be configured for GSLB.

The DNS server must be configured to delegate DNS requests for the subdomain in question to the load balancers; the load balancers’ GSLB services will serve the appropriate IP addresses to the DNS servers. Using the example presented throughout this section, the DNS server would be configured with a delegation for the domain quantum.example.com. The domain would be delegated to the load balancers.

Steps walking through creating a DNS delegation on a Microsoft DNS server in the context of setting up GSLB on our appliance can be found in the appendix, in the section Microsoft DNS Server Configuration.

8.5. Testing the Configuration
The configuration can be tested to make sure it’s working as expected.
From the command line on a Microsoft Windows machine, the `nslookup` program can be used to send test DNS queries to the load balancer(s). The primary load balancer is located at IP address 10.0.0.1 in the example presented here.

For the test, use the `-norecurse` option to instruct the load balancer **not** to attempt to query another server for the answer. A successful test would see the load balancer respond with the IP address of one of the online ActiveScale nodes, like so:

```
C:\Users\me>nslookup -norecurse quantum.example.com 10.0.0.1
Server: UnKnown
Address: 10.0.0.1

Name: quantum.example.com
Address: 10.0.0.11
```

9. Testing & Verification

For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

10. Technical Support

For more details about configuring the appliance and assistance with designing your deployment please don’t hesitate to contact the support team using the following email address: support@loadbalancer.org.

11. Further Documentation

For additional information, please refer to the Administration Manual.
12. Appendix

12.1. Microsoft DNS Server Configuration

Once the GSLB service has been fully configured on the primary load balancer at every site, as described in the previous sections, the DNS server at each site must be configured for GSLB.

The DNS server at each site must be configured to delegate DNS requests for the subdomain in question to the load balancers; the load balancers’ GSLB services will serve the appropriate IP addresses to the DNS servers. Using the example presented throughout this document, the DNS server at each site would be configured with a delegation for the domain `gslb.domain.tld`. The domain would be delegated to every load balancer across every site, which provides multi-site redundancy.

The exact steps for creating a DNS delegation vary between different DNS servers. Presented below are steps that walk through creating a DNS delegation on a Microsoft DNS server in the context of setting up GSLB on our appliance.

**Microsoft DNS Server**

Delegating a subdomain in Microsoft DNS Manager is a short process.

1. Open **DNS Manager** and create A records for every load balancer at every site, using **Action > New Host** (e.g. `dc1-lbprimary.domain.tld`, `dc1-lbsecondary.domain.tld`, `dc2-lbprimary.domain.tld`, and `dc2-lbsecondary`).

2. Provided that the load balancer part of the GSLB configuration has been completed and is working, the New Delegation wizard should now be used to delegate the subdomain to the load balancers. The delegation will use the new FQDNs for the load balancers, as defined in the previous step. The delegation wizard is located...
3. Test the delegation to make sure it is working as expected.

From the Windows command line, the `nslookup` program can be used to send test DNS queries to the DNS server. The DNS server is located at IP address 10.0.0.50 in the example presented here.

For the first test, use the `-norecurse` option to instruct the DNS server *not* to query another server for the answer. A successful test would see the DNS server respond and indicate that the subdomain in question is served by another server(s), giving the other server’s details, like so:

```
C:\Users\me>nslookup -norecurse gslb.domain.tld 10.0.0.50
Server: UnKnown
Address: 10.0.0.50

Name:   gslb.domain.tld
Served by:
```
For the second test, execute the same command **without** the `-norecurse` option. This should see the DNS server fetch the answer from the load balancer and then serve up the 'fetched' answer in its response. A successful test would see the server reply with the IP address of one of the online sites/services, like so:

```
C:\Users\me>nslookup gslb.domain.tld 10.0.0.50
Server: UnKnown
Address: 10.0.0.50

Non-authoritative answer:
Name:   gslb.domain.tld
Address: 10.0.0.2
```

12.2. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution.

We recommend that the Primary appliance is configured first and then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically replicated to the Secondary over the network using SSH/SCP.

**Note**

For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified – one for the VIP when it’s active on the Primary and one for the VIP when it’s active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

**Non-Replicated Settings**

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:
<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>

**Important**

Make sure that if these settings/updates have been configured on the Primary appliance, they’re also configured on the Secondary appliance.

**Adding a Secondary Appliance - Create an HA Clustered Pair**

**Note**

If you have already run the firewall lockdown wizard on either appliance, you’ll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

1. Deploy a second appliance that will be the Secondary and configure initial network settings.

2. Using the WebUI on the Primary appliance, navigate to: **Cluster Configuration > High-Availability Configuration**.
3. Specify the IP address and the loadbalancer user’s password for the Secondary (peer) appliance as shown in the example above.

4. Click Add new node.

5. The pairing process now commences as shown below:

6. Once complete, the following will be displayed on the Primary appliance:

7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.
Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

For more details on configuring HA with 2 appliances, please refer to [Appliance Clustering for HA](#).

For details on testing and verifying HA, please refer to [Clustered Pair Diagnostics](#).
13. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>11 August 2023</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
</tbody>
</table>
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.