# Table of Contents

1. About this Guide ......................................................... 3
2. Loadbalancer.org Appliances Supported .......................... 3
3. Loadbalancer.org Software Versions Supported ............... 3
4. Qumulo Hybrid File System Versions Supported ............. 3
5. Qumulo Hybrid File System ........................................ 3
6. Load Balancing Qumulo Hybrid File System .................... 3
   Load Balancing & HA Requirements ............................... 3
   Load Balancer Configuration ...................................... 3
   Connection Distribution ........................................... 4
   Health Checks ...................................................... 4
7. Deployment Concept .................................................. 4
   Explanation .......................................................... 5
8. Loadbalancer.org Appliance – the Basics ......................... 5
   Virtual Appliance .................................................. 5
   Initial Network Configuration .................................... 5
   Accessing the WebUI ............................................... 5
      Main Menu Options ............................................. 7
9. Appliance Configuration for Qumulo Hybrid File System ...... 8
   Step 1 – Configure the HA Pair .................................. 8
   Step 2 – Configure GSLB ......................................... 8
      Handling Multiple Subdomains, Including Wildcard Subdomains 8
      Appliance Configuration ....................................... 8
      DNS Server Configuration .................................... 11
      Testing the Configuration ..................................... 11
10. Microsoft DNS Server Configuration ............................. 12
    Microsoft DNS Server ........................................... 12
11. Testing & Verification ............................................... 15
    Accessing the Service .......................................... 15
12. Technical Support .................................................... 15
13. Further Documentation .............................................. 15
14. Conclusion .......................................................... 15
15. Appendix ........................................................... 16
    Configuring HA - Adding a Secondary Appliance ............... 16
       Non-Replicated Settings ..................................... 16
16. Document Revision History ....................................... 19
1. About this Guide

This guide details the steps required to configure a load balanced Qumulo Hybrid File System environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Qumulo 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 for load balancing Qumulo Hybrid File System. 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. Loadbalancer.org Software Versions Supported

- V8.4.1 or 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.

4. Qumulo Hybrid File System Versions Supported

- V3.0.0 or later

5. Qumulo Hybrid File System

Qumulo’s advanced hybrid file software allows you to symmetrically scale capacity and performance. Work in real-time, without the need for tree walks. Qumulo offers the most efficient file system in the industry, with the best raw-to-useable capacity that leverages 100 percent of useable storage.

Qumulo’s file system is built for the hybrid cloud, providing a single file solution whether your data is in the cloud or on-prem or scaling across both. Users can burst compute in AWS or GCP and shift primary workloads to the cloud without application changes.

6. Load Balancing Qumulo Hybrid File System

Note

It’s highly recommended that you have a working Qumulo environment first before implementing the load balancer.

Load Balancing & HA Requirements

The function of the load balancer is to ensure that connections to a Qumulo Hybrid file System cluster are distributed across healthy Qumulo nodes. This is done to provide a highly available and scalable service. To provide HA for the load balancer, Loadbalancer.org recommends that 2 appliances are deployed as an HA clustered pair.

Load Balancer Configuration

Load balancing a Qumulo deployment requires no Virtual Services (VIPs). Instead, both load balancers are
configured as smart DNS name servers for the FQDN of the Qumulo cluster address in question (qumulo.company.com in this guide). The is achieved using the load balancer’s built-in GSLB service and by using DNS delegation.

Connection Distribution
The GSLB service uses weighted round-robin load balancing to distribute inbound client connections across the healthy Qumulo nodes. The weights for the nodes can be set as required depending on relative node performance.

Health Checks
Each Qumulo node is regularly health-checked by each load balancer and this information is used when providing the smart DNS response to inbound DNS queries.

Note
For more details on configuring DNS delegation please refer to DNS Server Configuration for Qumulo Hybrid File System.

7. Deployment Concept
The diagram below illustrates how the load balancer is deployed.

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

**Explanation**

1. The client sends a DNS query for the service FQDN, e.g. qumulo.company.com to the local DNS server.
2. The local DNS server has the sub domain delegated to both load balancers (both load balancers are configured as name servers for the sub domain).
3. One of the load balancers receives the delegated DNS query.
4. The load balancer selects a healthy Qumulo node based on the GSLB health checks and the round robin algorithm used.
5. The load balancer returns the IP address of the selected Qumulo node to the DNS server.
6. The DNS server returns the IP address of the selected Qumulo node to the client.
7. The client connects directly to the Qumulo node.

**8. Loadbalancer.org Appliance – the Basics**

**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](#).

**Note**

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.

**Note**

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.

**Note**

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.

**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.

**Important**

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

**Accessing the WebUI**

The WebUI is accessed using a web browser. By default, user authentication is based on local Apache .htaccess files. User administration tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.

**Note**

A number of compatibility issues have been found with various versions of Internet Explorer and
1. Using a browser, access the WebUI using the following URL:


2. Log in to the WebUI:

   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. If you click **Accept** the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simple click **Dismiss**.

**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
9. Appliance Configuration for Qumulo Hybrid File System

Step 1 – Configure the HA Pair

If you intend to deploy 2 load balancers in order to configure an HA clustered pair (our recommended configuration) then the HA pair should be configured first before the GSLB configuration takes place. This simplifies the process since GSLB settings will then be automatically replicated to the paired appliance. This helps ensure that both appliances are correctly configured and ready for sub domain delegation (please refer to [DNS Server Configuration for Qumulo Hybrid File System]).

Once the HA pair is configured, the remaining configuration should take place on the Primary unit, the Secondary unit will then be kept in sync automatically. For details on configuring an HA pair, please refer to Configuring HA - Adding a Secondary Appliance.

Step 2 – Configure GSLB

Handling Multiple Subdomains, Including Wildcard Subdomains

Scenario

Object storage-related DNS configurations may use various DNS subdomains, for example:

- s3-<region/location>.domain.tld (e.g. s3-region1.domain.tld)

Some scenarios also require the use of wildcard DNS entries, for example to cover bucket specific subdomains like app-instance-f57ac0.s3-region1.domain.tld.

Solution

Configuring DNS delegation can be complex. As such, the supported solution is to:

- Delegate a single subdomain to the load balancer, e.g. gslb.
- Use CNAME records to point everything else at the delegated subdomain

For example, the subdomain gslb.domain.tld would be delegated and everything else would point to it. This would look like so:

<table>
<thead>
<tr>
<th>DNS Entry</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>gslb.</td>
<td>Delegate to the load balancer</td>
</tr>
<tr>
<td>s3-&lt;region&gt;.</td>
<td>CNAME to gslb.domain.tld</td>
</tr>
<tr>
<td>*.s3-&lt;region&gt;</td>
<td>CNAME to gslb.domain.tld</td>
</tr>
<tr>
<td>s3-admin-console.</td>
<td>CNAME to gslb.domain.tld</td>
</tr>
</tbody>
</table>

This approach simplifies DNS entry configuration, particularly when wildcard entries are involved.

Appliance Configuration

The GSLB service should be configured on the primary load balancer appliance and should be configured at each site if a multi-site deployment is being configured.

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. `gslb.domain.tld`

   **Note**

   If only working with a single subdomain then it’s perfectly acceptable to directly delegate the specific subdomain in question, e.g. `s3-region1.domain.tld`, rather than delegating a generic subdomain like `gslb.domain.tld`.

5. Define the Hostname of what will be the delegated subdomain, e.g. `gslb.domain.tld`
6. Click Submit.

Step 2 – Configure the Members

Each member is a single Qumulo node.

1. Select the Members tab.
2. Click the New Member button.
3. Enter a friendly Name for the member, e.g. `qumulo-node1`.
4. Specify an IP address for the member: in this context, this should be the IP address of the Qumulo 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 Qumulo 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 `gslb.domain.tld` with the members (Qumulo nodes), all of which should serve Qumulo traffic.

1. Select the **Pools** tab.
2. Click the **New Pool** button.
3. Enter a friendly *Name* for the pool, e.g. `qumulo-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. `gslb.domain.tld`.
8. In the *Members* section, drag the appropriate members (Qumulo 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.

DNS Server Configuration
Once the GSLB service has been configured on the primary load balancer at every site, the DNS server at each site must then 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 section, 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.

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.

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 Qumulo nodes, like so:

```
C:\Users\me>nslookup -norecurse gslb.domain.tld 10.0.0.1
Server: UnKnown
Address: 10.0.0.1
Name: gslb.domain.tld
Address: 10.0.0.11
```

10. **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 at **Action > New Delegation**.
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:
   - dc1-lbprimary.domain.tld 10.0.0.100
gslb.domain.tld
   - dc1-lbsecondary.domain.tld 10.0.0.101
gslb.domain.tld
   - dc2-lbprimary.domain.tld 172.16.0.100
gslb.domain.tld
   - dc2-lbsecondary.domain.tld 172.16.0.101
gslb.domain.tld
   ```

   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
   ```
11. Testing & Verification

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

Since the load balancers have no Virtual Services, there is no graphical overview of ‘healthy’ services to check and verify on the System Overview page of the WebUI. Instead, the GSLB configuration should be checked, ensuring that the client is able to resolve the FQDN of the Qumulo deployment via delegation and connect to a healthy Qumulo node.

See the earlier section Testing the Configuration for instructions on how to test the GSLB setup.

Accessing the Service

A successful test will see the test connection passed directly from the test client to one of the online Qumulo nodes.

12. 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.

13. Further Documentation


14. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Qumulo Hybrid File System environments.
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 should be configured first, 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.

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 Configuration</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 Configuration</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.

To add a Secondary node - i.e. create a highly available clustered pair:
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 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 blue message box at the top of the screen.

**Note** Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

**Note** For more details on configuring HA with 2 appliances, please refer to **Appliance Clustering for HA**.

**Note** For details on testing and verifying HA, please refer to **Clustered Pair Diagnostics**.
# 16. 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>23 April 2020</td>
<td>First draft</td>
<td></td>
<td>RJC</td>
</tr>
<tr>
<td>1.0.1</td>
<td>29 April 2020</td>
<td>Various minor updates</td>
<td>Improved readability</td>
<td>RJC</td>
</tr>
<tr>
<td>1.0.2</td>
<td>3 September 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td>1.1.0</td>
<td>1 December 2021</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</td>
</tr>
<tr>
<td>1.2.0</td>
<td>6 April 2022</td>
<td>Updated GSLB set up instructions to use GUI-driven GSLB configuration</td>
<td>GSLB updates across all documentation Changed to use new, consistent common component</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.