# 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
   Step 3 – Apply the GSLB Configuration ............................... 9
   Step 4 – Verify the GSLB Configuration .............................. 9
10. DNS Server Configuration for Qumulo Hybrid File System ........ 10
   Microsoft DNS Server ....................................................... 10
11. Testing & Verification .......................................................... 11
   Verify the DNS Delegation ............................................... 11
   Verify the Full DNS Request & Response ............................ 11
   Accessing the Service ....................................................... 12
12. Technical Support .............................................................. 12
13. Further Documentation ........................................................ 12
14. Conclusion ........................................................................... 12
15. Appendix ............................................................................. 13
   Configuring HA - Adding a Secondary Appliance ............... 13
16. Document Revision History .................................................. 16
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

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 The Virtual Appliance - Hypervisor Deployment and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Note

For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.

Initial Network Configuration

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway, DNS 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. Appliance authentication is based on Apache .htaccess files. User admin tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.
A number of compatibility issues have been found with various versions of Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

If required, users can also be authenticated against LDAP, LDAPS, Active Directory or Radius. For more information please refer to External Authentication.

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>

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

Once logged in, the WebUI will be displayed as shown below:
Note: The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.

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, 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
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

Using the WebUI of the Primary appliance, navigate to Cluster Configuration > GSLB Configuration and select Polaris Config from the drop-down list.

If GSLB has never been configured, the default example configuration will be displayed in the text box.

The example below relates to the 4-node example presented in section 7. This can be copied and pasted to replace the default example and can be used as a basis for creating a deployment-specific configuration.

The elements highlighted in bold should be customised to reflect the Qumulo deployment in question. Stanzas should be added or removed as needed under the "members" section to reflect your deployment.

Be sure to click the Update button when finished to write the configuration to disk.

Note

Indentation is important and must be preserved, otherwise the underlying Polaris GSLB service will throw an error.
globalnames:
  qumulo.company.com:
    pool: qumulo-nodes
    ttl: 5

pools:
  qumulo-nodes:
    monitor: tcp
    monitor_params:
      port: 443
      timeout: 2
      interval: 5
      retries: 2
    lb_method: wrr
    fallback: any
    members:
      - ip: 10.0.0.11
        name: qumulo-node1
        weight: 1
      - ip: 10.0.0.12
        name: qumulo-node2
        weight: 1
      - ip: 10.0.0.13
        name: qumulo-node3
        weight: 1
      - ip: 10.0.0.14
        name: qumulo-node4
        weight: 1

Note The GSLB configuration presented above does not include any Qumulo floating IP addresses. To aid a graceful failover, these addresses can also be added to the GSLB configuration.

Step 3 – Apply the GSLB Configuration
If updating an existing GSLB configuration then simply click the Reload GSLB button when prompted.

If setting up the GSLB service for the first time, the service must undergo a full restart (rather than a reload) for the configuration to be applied. To do this, using the WebUI, navigate to Maintenance > Restart Services and click the Restart GSLB button. For an HA pair, this procedure to restart the service (rather than reload) must also be carried out on the Secondary appliance.

For any subsequent configuration updates, the GSLB service only needs to be reloaded using the service reload link presented at the top of the WebUI on the Primary appliance after changes have been.

Step 4 – Verify the GSLB Configuration
The GSLB configuration should be tested to ensure it’s working as expected and that both Primary and Secondary appliances are able to correctly respond to DNS queries for the sub domain. This must be operating correctly when configuring the DNS delegation in the following section.

From a Windows command prompt, the nslookup command can be used to send test DNS queries to the load balancers. 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 as shown below:
This test should be repeated using the IP address of the Secondary unit to ensure that the Secondary is also able to return the IP address of one of the online Qumulo nodes.

10. DNS Server Configuration for Qumulo Hybrid File System

Once the load balancer’s GSLB service has been fully configured and tested as described in the previous section, the local DNS server must also 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 balancer’s GSLB services will then serve the IP address of the selected Qumulo node to the DNS server. Using the example presented throughout this document, the DNS server must be configured with a delegation for the sub domain **qumulo.company.com**. The sub domain must be delegated to both load balancers if using an HA pair.

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 the load balancer.

**Microsoft DNS Server**

Delegating a subdomain using Microsoft DNS Manager is a straightforward process:

1. Open **DNS Manager** and create A records for each load balancer using the menu option: *Action > New Host*. (e.g. *lbmaster.company.com*, IP **10.0.0.1** and *lbslave.company.com*, IP **10.0.0.2** for an HA pair of load balancers).

![DNS Manager](image)

2. Provided that the load balancer’s GSLB configuration has been completed and tested as described in **DNS Server Configuration for Qumulo Hybrid File System**, the **New Delegation** wizard can now be used to delegate the chosen subdomain (in this guide **qumulo.company.com**) to the load balancers. The delegation wizard can be started using the menu option: *Action > New Delegation*.

Now add each load balancer as a name server for the sub domain as shown below:
11. Testing & Verification

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.

Verify the DNS Delegation

From a Windows command prompt, the `nslookup` command 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 this 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 other name servers, giving the other server’s details as shown in the example below:

```
C:\Users\me>nslookup -norecurse qumulo.company.com 10.0.0.50
Server: UnKnown
Address: 10.0.0.50

Name: qumulo.company.com
Served by:
- lbmaster.company.com
  10.0.0.1 + qumulo.company.com
- lbslave.company.com
  10.0.0.2 qumulo.company.com
```

Verify the Full DNS Request & Response

Now execute the same command without the `-norecurse` option. This should see the DNS server fetch the answer from one of the load balancers 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 Qumulo nodes as shown in the example below:
C:\Users\me>nslookup qumulo.company.com 10.0.0.50
Server: UnKnown
Address: 10.0.0.50
Non-authoritative answer:
Name: qumulo.company.com
Address: 10.0.0.11

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.
15. Appendix

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.

**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.

**Note**

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,</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>Firewall connection tracking table size, NIC offloading, SMTP relay,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
<td>Appliance management lockdown settings</td>
</tr>
<tr>
<td></td>
<td>Wizard</td>
<td></td>
</tr>
</tbody>
</table>

To add a Secondary node - i.e. create a highly available clustered pair:
1. Deploy a second appliance that will be the Secondary and configure initial network settings.

2. Using the WebUI, 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:
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](#).
## 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>
</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.