1. About this Guide
This guide details the steps required to configure a load balanced MinIO Server environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any MinIO Server 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 MinIO. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td>Enterprise R320</td>
<td>Enterprise 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products/hardware](http://www.loadbalancer.org/products/hardware)
** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- V8.3.4 and later

4. MinIO Software Versions Supported

- MinIO Server – all versions

5. MinIO Server
MinIO Server is a high performance open source S3 compatible object storage system designed for hyper-scale private data infrastructure.

MinIO can be installed on a wide range of industry standard hardware. It can run as a standalone server, but it's full power is unleashed when deployed as a cluster with multiple nodes. From 4 to 32 nodes and beyond using MinIO federation.
Data is protected against hardware failure and data corruption using erasure code at the object level and bitrot protection. MinIO is highly available – a distributed cluster can lose up to half the disks on a single node and up to half the nodes and continue to serve objects.

The use of the **Strict Consistency** data model ensures that an exact copy of all data is available from all nodes. With **Eventual Consistency**, read operations could return old or stale data.

MinIO integrates with various authentication systems such as WSO2, OKTA and Active Directory to authenticate applications and users. Data integrity is ensured using encryption and tamper proofing technology.

**Operating Modes**

MinIO Server supports the following modes of operation:

- **Standalone** – runs on a single node with a single disk or for improved resilience a RAID array
- **Standalone Erasure Code** – runs on a single node: object data and parity is striped across all drives in that node
- **Distributed Erasure Code** – runs on multiple nodes: object data and parity is striped across all disks in all nodes, all objects are accessible from any working node

---

**Note:** RAID is not required for the second and third options. Data is protected using object level erasure coding and bitrot protection.

---

6. **Load Balancing MinIO Server**

**MinIO Configuration**

**Operating Mode**

To create a MinIO cluster that can be load balanced, MinIO must be deployed in **Distributed Erasure Code** mode. This enables multiple disks across multiple nodes to be pooled into a single object storage server. Object data and parity is striped across all disks in all nodes. All objects can then be accessed from any node in the cluster.

Using a load balancer ensures that connections are only sent to ready/available nodes and also that these connections are distributed equally.

**Load Balancer Configuration**

**Operating Mode**

The load balancer is deployed at Layer 7. This mode offers high performance and requires no configuration changes to the load balanced MinIO Servers.

**Timeouts**

For MinIO Server, the load balancer’s client and server timeouts are set to 10 minutes.
Port Requirements

The following table shows the port(s) that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>9000</td>
<td>TCP</td>
<td>MinIO communications</td>
</tr>
</tbody>
</table>

Note: Port 9000 is the default port for MinIO but this can be changed if required by modifying the node startup command – see page 8 for more details.

SSL/TLS Termination

To enable secure communication, SSL/TLS is terminated on the load balancer.

Health Checks

As mentioned here, MinIO includes 2 un-authenticated probe points that can be used to determine the state of each MinIO node. In this guide, the heath checks are configured to read the readiness probe /minio/health/ready.

Deployment Concept

VIPs = Virtual IP Addresses

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 section 1 in the appendix on page 14 for more details on configuring a clustered pair.
Virtual Appliance Download & Deployment
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 and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB 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.

Initial Network Configuration
The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

Method 1 - Using the Network Setup Wizard at the console
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

Method 2 - Using the WebUI
Using a browser, connect to the WebUI on the default IP address/port: https://192.168.2.21:9443
To set the IP address & subnet mask, use: Local Configuration > Network Interface Configuration
To set the default gateway, use: Local Configuration > Routing
To configure DNS settings, use: Local Configuration > Hostname & DNS

Accessing the Web User Interface (WebUI)
The WebUI can be accessed via HTTPS at the following URL: https://192.168.2.21:9443/lbadmin
* Note the port number → 9443

(replace 192.168.2.21 with the IP address of your load balancer if it’s been changed from the default)
Login using the following credentials:
Username: loadbalancer
Password: loadbalancer

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

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

---

HA Clusted 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 slave unit is covered in section 1 of the appendix on page 14.
8. Running MinIO in Distributed Erasure Code Mode

The test lab used for this guide was built using 4 Linux nodes, each with 2 disks:

1. For nodes 1 – 4:

   ◦ set the hostnames using an appropriate sequential naming convention, e.g. `minio1, minio2, minio3, minio4`
   ◦ mount the disks using an appropriate sequential naming convention, e.g.
     - disk 1 → `/mnt/minio-data1`
     - disk 2 → `/mnt/minio-data2`
   ◦ ensure that `/etc/hosts` refers to the node’s allocated IP address rather than the 127.0.0.1 loopback address
   ◦ set the domain name of each node to an appropriate value, e.g. `lbtestdom.com`

2. Run the following commands on all nodes to start MinIO in Distributed Erasure Code mode:

```bash
export MINIO_ACCESS_KEY=<minio>
export MINIO_SECRET_KEY=<minio123>
./minio server http://minio{1...4}.lbtestdom.com:9000/mnt/minio-data{1...2}
```

Note: The sequential naming convention used for the hostnames and the disks enables this command format to be used.

Note: Change the hostnames, domain name, access key and secret key to suit your requirements.

9. Appliance Configuration for MinIO

a) Layer 7 VIP Configuration

1. Using the web user interface, navigate to `Cluster Configuration > Layer 7 – Virtual Services` and click on Add a new Virtual Service
2. Enter the following details:

![VIP configuration interface]

3. Enter an appropriate name for the VIP in the Label field, e.g. MinIO-Cluster
4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.110.65
5. Set the Virtual Service Ports field to 9000
6. Set the Layer 7 Protocol to HTTP Mode
7. Click Update
8. Now click Modify next to the newly created VIP
9. Scroll down to the Persistence section and set Persistence Mode to None
10. Scroll down to the Health Checks section and set the Health Check to Negotiate HTTP (HEAD)
11. Set Request to Send to minio/health/ready

Note: If preferred, the liveness probe (minio/health/live) can be used instead of the readiness probe (minio/health/ready). For more details of both please refer to the MinIO monitoring documentation available here.

12. Leave Response Expected blank – this will cause the load balancer to look for an HTTP 200 OK response from each Real Server
13. Scroll down to the Other section and click [Advanced]
14. Enable (check) the Timeout checkbox and set both Client Timeout & Real Server Timeout to 10m (i.e. 10 minutes)
15. Click Update

b) Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Real Servers and click on Add a new
Real Server next to the newly created MinIO-Cluster VIP

2. Enter an appropriate name for the server in the Label field, e.g. minio1
3. Change the Real Server IP Address field to the required IP address, e.g. 192.168.110.60
4. Set the Real Server Port field to 9000
5. Click Update
6. Now repeat these steps to add the other MinIO server nodes

c) Upload Your SSL Certificate to The Load Balancer

To upload a Certificate:

1. Using the WebUI, navigate to: Cluster Configuration > SSL Certificates
2. Click Add a new SSL Certificate & select Upload prepared PEM/PFX file

3. Enter a suitable Label (name) for the certificate, e.g. MinIO-Cert
4. Browse to and select the certificate file to upload (PEM or PFX format)
5. Enter the password (if applicable)
6. Click Upload Certificate – if successful a message similar to the following will be displayed:
d) Configure SSL Termination

1. Using the WebUI, navigate to: Cluster Configuration > SSL Termination and click **Add a new Virtual Service**

![Virtual Service Configuration](image)

2. Enter a suitable Label (name) for the VIP, e.g. **Minio-SSL**
3. Set **Associated Virtual Service** to the Layer 7 VIP created previously, e.g. **MinIO-Cluster**
4. Leave **SSL Certificate** set to **Default Self Signed Certificate** or select the certificate you've just uploaded depending on your requirements
5. Click **Update**

e) Finalizing the Configuration

To apply the new settings, reload HAProxy & Stunnel using the buttons in the blue box at the top of the screen.

10. Testing & Verification

Once the load balancer and MinIO nodes are configured you can use the MinIO client, a web browser or an alternative 3rd party S3 browser to view the buckets and objects. Connect to the VIP address on the load balancer rather than one of the MinIO nodes

Using System Overview

The System Overview can be viewed using the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the MinIO nodes) and shows the state/health of each node as well as the state of the cluster as a whole. This can be used to ensure all servers are up and available (green).
Obtaining information about the MinIO Nodes

# set an alias for the service using mc
./mc config host add myminio http://192.168.110.60:9000 minio minio123

# get minio server information for all nodes
./mc admin info server myminio

- minio1.lbtestdom.com:9000
  Uptime: 43 minutes
  Version: 2019-10-11T00:38:09Z
  Storage: Used 901 MiB, Free 24 GiB
  Drives: 2/2 OK
  
  CPU	min	avg	max
  current	0.03%	0.04%	0.04%
  historic	0.02%	0.17%	42.67%

  MEM	usage
  current	68 MiB
  historic	68 MiB

- minio2.lbtestdom.com:9000
  Uptime: 43 minutes
  Version: 2019-10-11T00:38:09Z
  Storage: Used 901 MiB, Free 24 GiB
  Drives: 2/2 OK
  
  CPU	min	avg	max
  current	0.04%	0.04%	0.04%
  historic	0.02%	0.07%	3.42%

  MEM	usage
  current	68 MiB
  historic	68 MiB

- minio3.lbtestdom.com:9000
  Uptime: 43 minutes
  Version: 2019-10-11T00:38:09Z
  Storage: Used 901 MiB, Free 24 GiB
  Drives: 2/2 OK
  
  CPU	min	avg	max
  current	0.02%	0.02%	0.03%
  historic	0.02%	0.09%	5.44%

  MEM	usage
  current	68 MiB
  historic	68 MiB

- minio4.lbtestdom.com:9000
  Uptime: 43 minutes
  Version: 2019-10-11T00:38:09Z
  Storage: Used 901 MiB, Free 24 GiB
11. 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.

12. Further Documentation

13. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced MinIO Server environments.
14. Appendix

1 - Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

Note: A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
- Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
- SNMP settings
- Graphing settings
- Firewall Script & Firewall Lockdown Script settings
- Software updates

To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration

![Create a Clustered Pair](image-url)
• Specify the IP address and the loadbalancer users password (the default is ‘loadbalancer’) for the slave (peer) appliance as shown above

• Click Add new node

• The pairing process now commences as shown below:

Once complete, the following will be displayed:

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 master appliance will also automatically restart heartbeat on the slave appliance.

Note: Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
## 15. 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>16th October 2019</td>
<td>First draft</td>
<td></td>
<td>RJC</td>
</tr>
<tr>
<td>1.0.1</td>
<td>29th October 2019</td>
<td>Expanded note on parameters to be customised in the MinIO startup command</td>
<td>To remind the reader to change the command to suit their environment</td>
<td>RJC</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.

**United Kingdom**
Loadbalancer.org Ltd.
Compass House, North Harbour Business Park, Portsmouth, PO6 4PS
UK:+44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

**United States**
Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

**Canada**
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver,
BCV6B 2Z4, Canada
TEL:+1 302.213.0122
sales@loadbalancer.org
support@loadbalancer.org

**Germany**
Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org