Table of Contents

1. About this Guide ......................................................... 3
2. Loadbalancer.org Appliances Supported .................................. 3
3. Loadbalancer.org Software Versions Supported .......................... 3
4. MinIO Software Versions Supported ...................................... 3
5. MinIO Server .............................................................. 3
   Operating Modes ....................................................... 3
6. Load Balancing MinIO Server .............................................. 4
   MinIO Configuration .................................................... 4
      Operating Mode ....................................................... 4
   Load Balancer Configuration ......................................... 4
      Operating Mode ....................................................... 4
      Timeouts ............................................................. 4
      Port Requirements .................................................. 4
      SSL/TLS Termination ............................................... 4
      Health Checks ....................................................... 4
      Deployment Concept .............................................. 4
7. Loadbalancer.org Appliance – the Basics ................................ 5
   Virtual Appliance ...................................................... 5
   Initial Network Configuration ....................................... 5
   Accessing the WebUI .................................................. 6
      Main Menu Options ................................................. 7
   HA Clustered Pair Configuration ................................... 8
8. Running MinIO in Distributed Erasure Code Mode .................... 8
9. Appliance Configuration for MinIO ...................................... 8
   a) Layer 7 VIP Configuration ....................................... 8
   b) Defining the Real Servers (RIPs) ................................ 9
   c) Upload Your SSL Certificate to The Load Balancer ............. 10
   d) Configure SSL Termination ...................................... 10
   e) Finalizing the Configuration .................................... 11
10. Testing & Verification ................................................... 11
    Using System Overview ............................................. 11
    Obtaining information about the MinIO Nodes ..................... 12
11. Technical Support ..................................................... 13
12. Further Documentation ................................................ 13
13. Conclusion ............................................................. 13
14. Appendix ............................................................... 14
    Configuring HA - Adding a Secondary Appliance ............... 14
       Non-Replicated Settings ......................................... 14
15. Document Revision History ............................................ 17
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. 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

- V8.3.8 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.

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 loose 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 additional 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 Running MinIO in Distributed Erasure Code Mode 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 health 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 Configuring HA - Adding a Secondary Appliance for more details on configuring a clustered pair.

7. 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 Edge. The WebUI has been tested and verified using both Chrome & Firefox.

**Note**

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>

   **Note**

   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
- **Logs** - View various appliance logs
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 Configuring HA - Adding a Secondary Appliance.

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 nodes own 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:

   ```
   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:
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:

   *Information: cert1 SSL Certificate uploaded successfully.*

d) **Configure SSL Termination**

1. Using the WebUI, navigate to: **Cluster Configuration > SSL Termination** and click **Add a new Virtual Service**.
2. Using the Associated Virtual Service drop-down, select the Virtual Service created above, e.g. MinIO-Cluster.

Note: Once the VIP is selected, the Label field will be auto-populated with SSL-MinIO-Cluster. This can be changed if preferred.

3. Ensure that the Virtual Service Port is set to 443.
5. Select the required SSL Certificate.
6. Click Update.

**e) Finalizing the Configuration**

To apply the new settings, HAProxy and STunnel must both be reloaded. This can be done using the buttons in the blue box at the top of the screen or by using the Restart Services menu option:

1. Using the WebUI, navigate to: Maintenance > Restart Services.
2. Click Reload HAProxy.
3. Click Reload STunnel.

**10. Testing & Verification**

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

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
  - Drives: 2/2 OK
  - CPU min avg max
    - current 0.02% 0.03% 0.03%
    - historic 0.02% 0.07% 15.33%
  - MEM usage
    - current 68 MiB
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

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.

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:*
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]*.
## 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>16 October 2019</td>
<td>First draft</td>
<td></td>
<td>RJC</td>
</tr>
<tr>
<td>1.0.1</td>
<td>29 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>
<tr>
<td>1.0.2</td>
<td>2 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>1.1.1</td>
<td>26 April 2022</td>
<td>Updated SSL related content to reflect latest software version</td>
<td>New software release</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.