LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing MinIO Server

Version 1.2.0

Table of Contents

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/enterprise.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

> **Note** The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. MinIO

- All versions

4. 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.

4.1. 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 in not required for the second and third options. Data is protected using object level erasure coding and bitrot protection.

5. Load Balancing MinIO Server

5.1. MinIO Configuration

5.1.1. 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.

5.2. Load Balancer Configuration

5.2.1. Operating Mode

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

5.2.2. Timeouts

For MinIO Server, the load balancer's client and server timeouts are set to 1 0 minutes.

5.2.3. Port Requirements

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

Port	Protocols	Use
9000	TCP	MinIO communications

> **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.

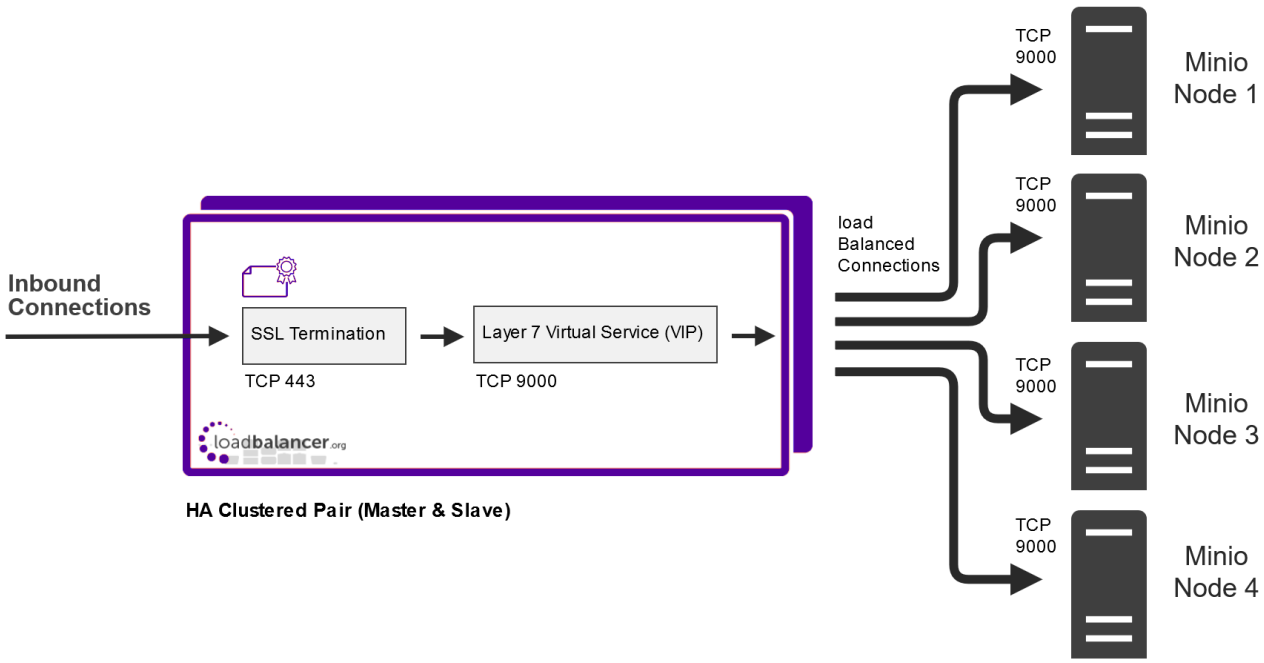
5.2.4. SSL/TLS Termination

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

5.2.5. 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**.

5.2.6. Deployment Concept



VIP = **V**irtual **IP** Address

> **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.

6. Loadbalancer.org Appliance – the Basics

6.1. 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.

> **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.

6.2. Initial Network Configuration

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

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

6.3. 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.

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

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

   https://<IP-address-configured-during-the-network-setup-wizard>:9443/lbadmin/

   > **Note** You'll receive a warning about the WebUI's SSL certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

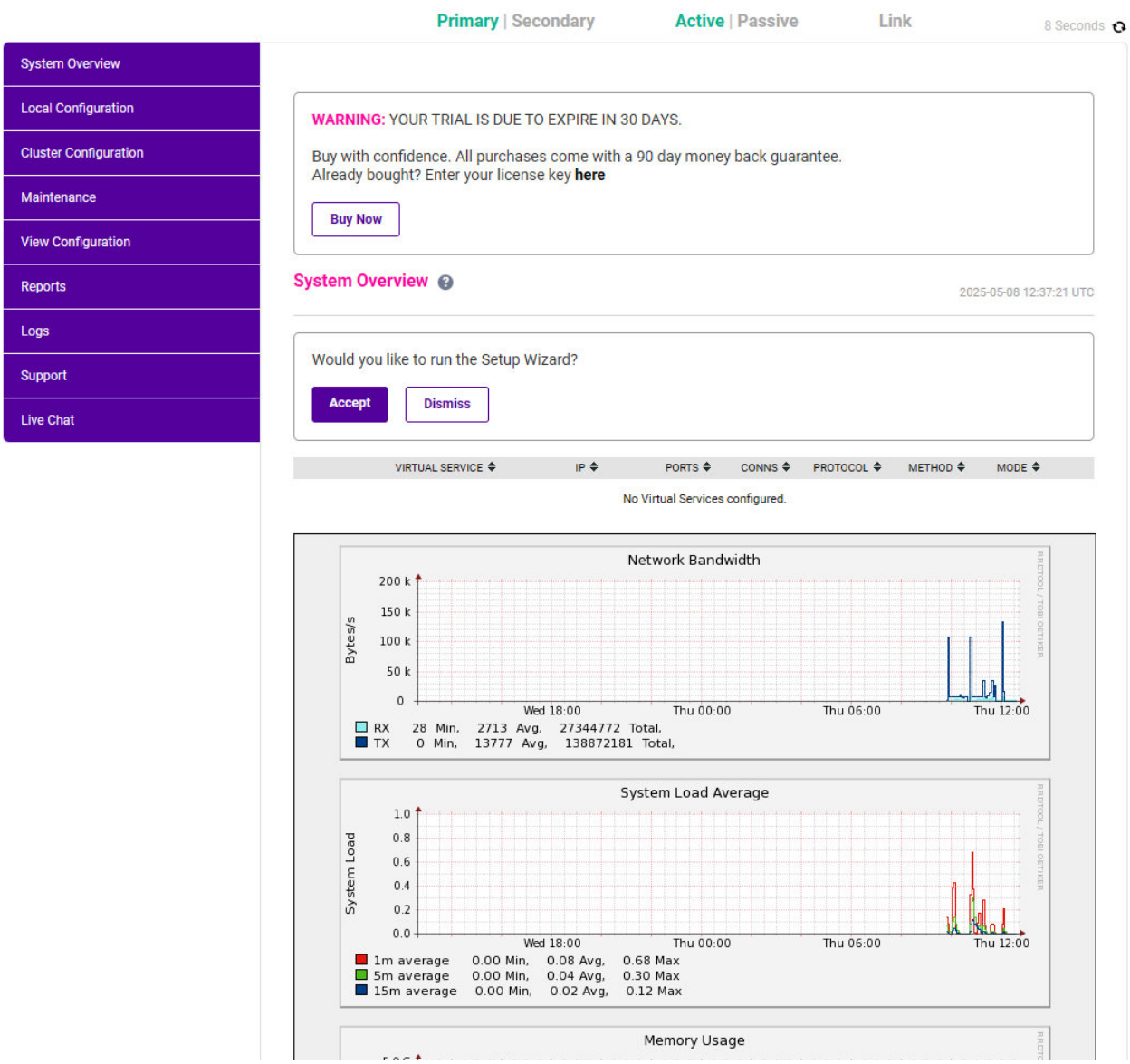
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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.

> **Note** The Setup Wizard can only be used to configure Layer 7 services.

6.3.1. 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 creating 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

6.4. Appliance Software Update

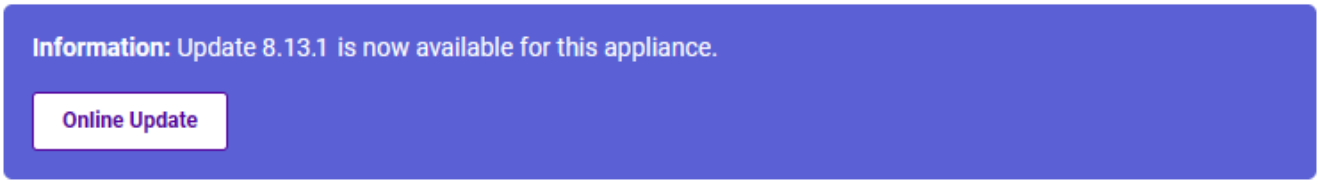
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **Note** For full details, please refer to Appliance Software Update in the Administration Manual.

> **Note** Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

6.4.1. Online Update

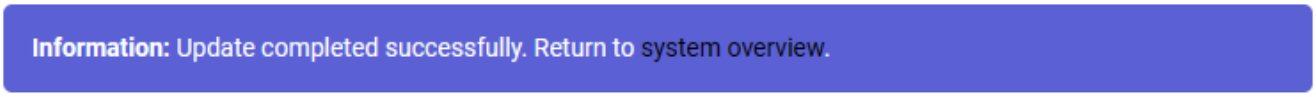
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

> **Important** Do not navigate away whilst the update is ongoing, this may cause the update to fail.

The update can take several minutes depending on download speed and upgrade version. Once complete, the following message will be displayed:



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

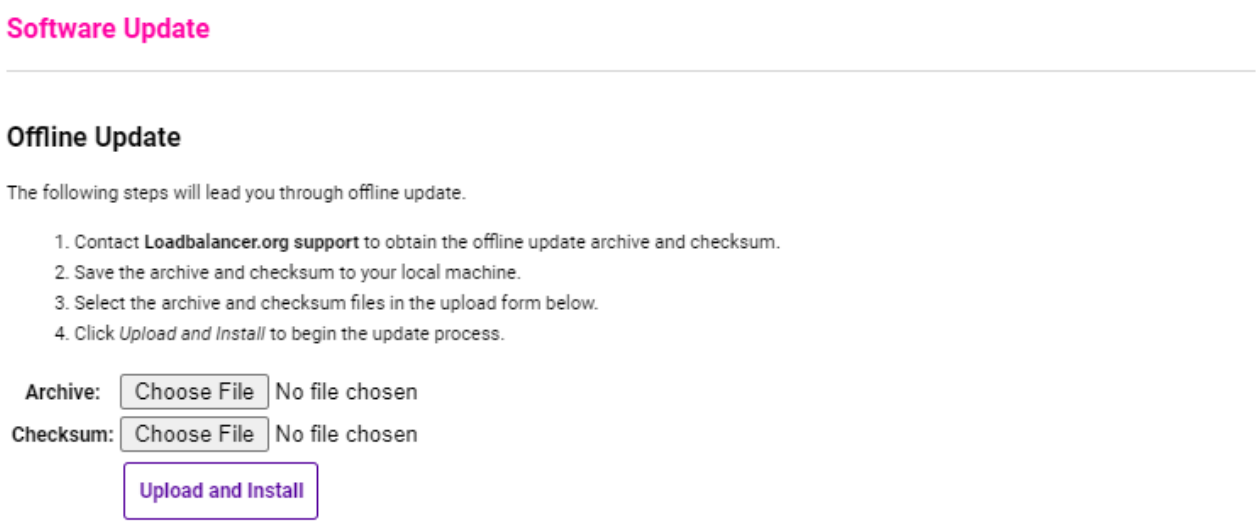
6.4.2. Offline Update

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

To check for the latest version, please refer to our product roadmap page available here. To obtain the latest offline update files contact support@loadbalancer.org.

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:



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.

6.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

Protocol	Port	Purpose
TCP	22 *	SSH
TCP & UDP	53 *	DNS / GSLB
TCP & UDP	123	NTP
TCP & UDP	161 *	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page
TCP	9443 *	WebUI - HTTPS
TCP	25565 *	Shuttle service (Centralized/Portal Management)

> **Note** The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket

Addresses.

6.6. 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 Configuring HA - Adding a Secondary Appliance.

7. 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}
```

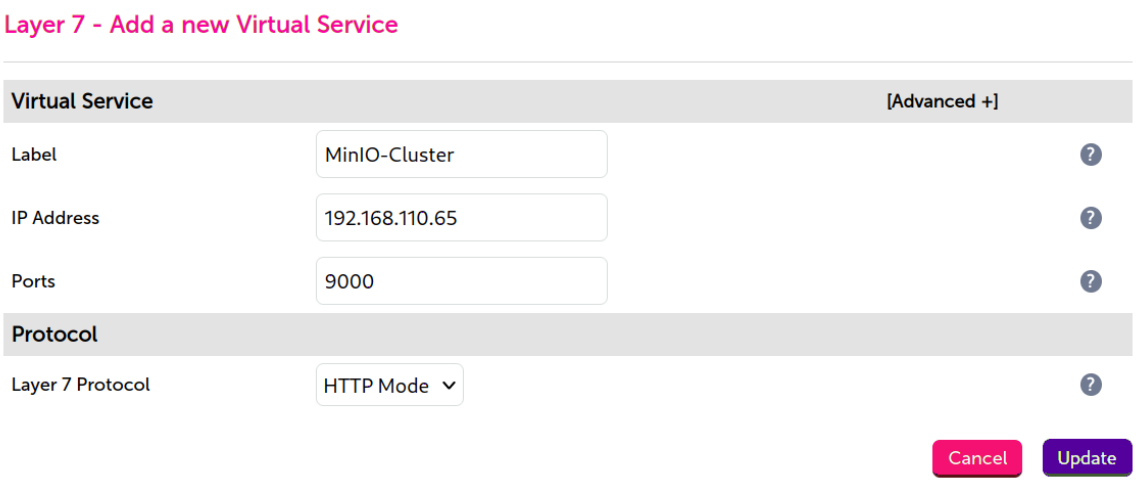
> **Note** The sequential naming convention used for the hostnames and the disks enables this command format to be used.

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

8. Appliance Configuration for MinIO

8.1. 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:



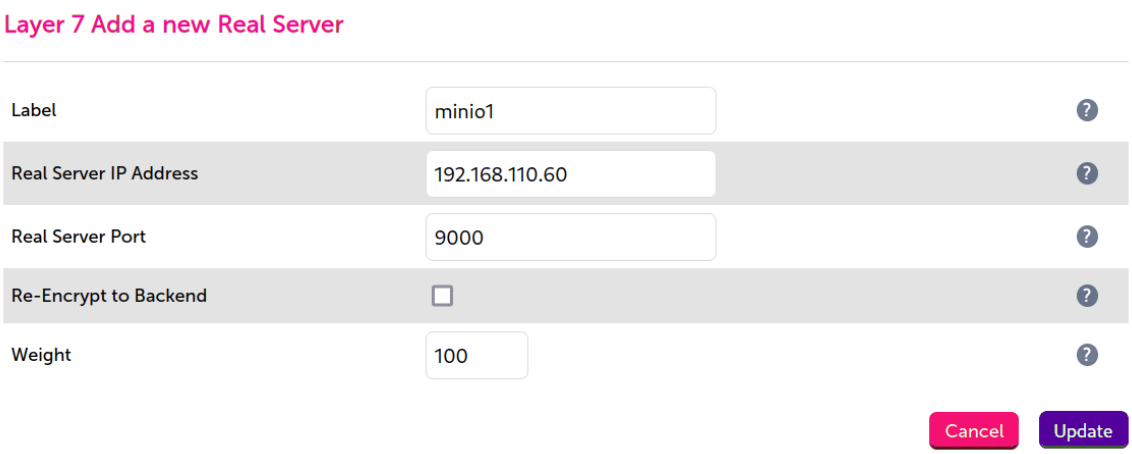
3. Enter an appropriate name for the VIP in the *Label* field, e.g. **MinIO-Cluster**.
4. Set the *Virtual Service IP* address field to the required IP address, e.g. **192.168.110.65**.
5. Set the *Virtual Service Ports* field to **9000**.
6. Set the *Layer 7 Protocol* to **HTTP Mode**.
7. Click **Update**.
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**.

8.2. 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.

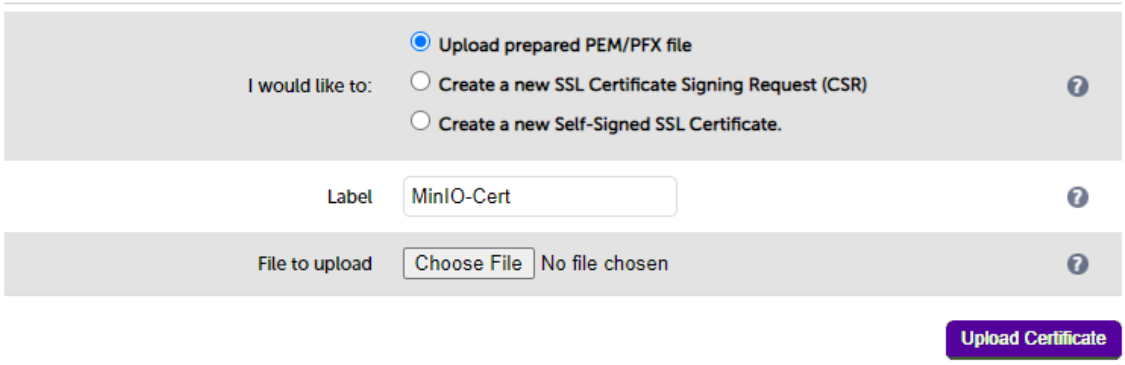


2. Enter an appropriate name for the server in the *Label* field, e.g. **minio1**.
3. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.110.60**.
4. Set the *Real Server Port* field to **9000**.
5. Click **Update**.
6. Now repeat these steps to add the other MinIO server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

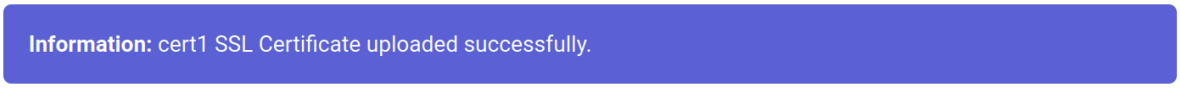
8.3. c) Upload Your SSL Certificate to The Load Balancer

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*.

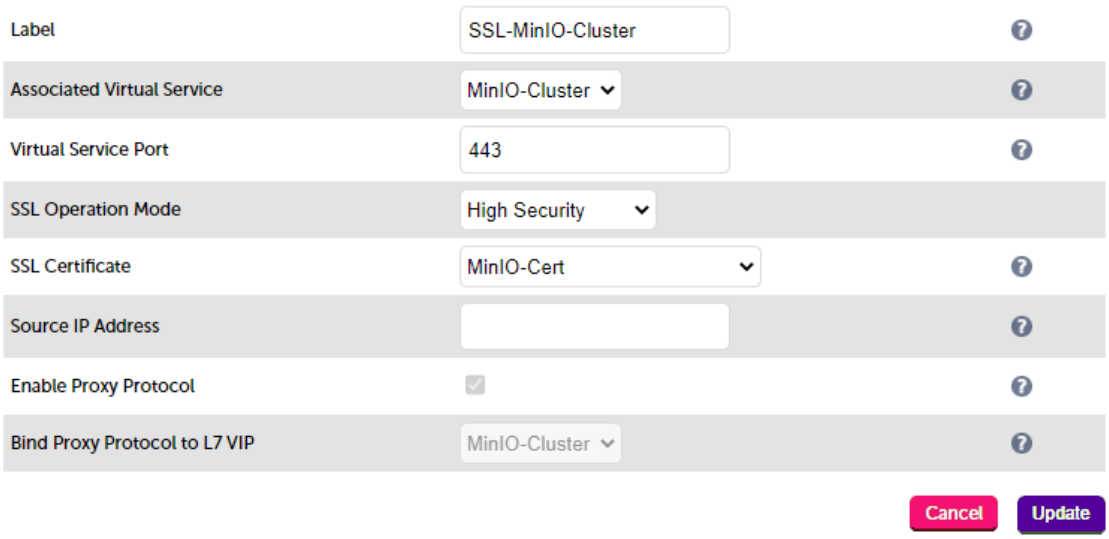


3. Enter a suitable *Label* (name) for the certificate, e.g. **MinIO-Cert**.
4. Browse to and select the certificate file to upload (PEM or PFX format).
5. Enter the password (if applicable).
6. Click **Upload Certificate** – if successful, a message similar to the following will be displayed:



8.4. 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**.
4. Leave *SSL Operation Mode* set to **High Security**.
5. Select the required *SSL Certificate*.
6. Click **Update**.

8.5. 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 "Commit changes" 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**.

9. Testing & Verification

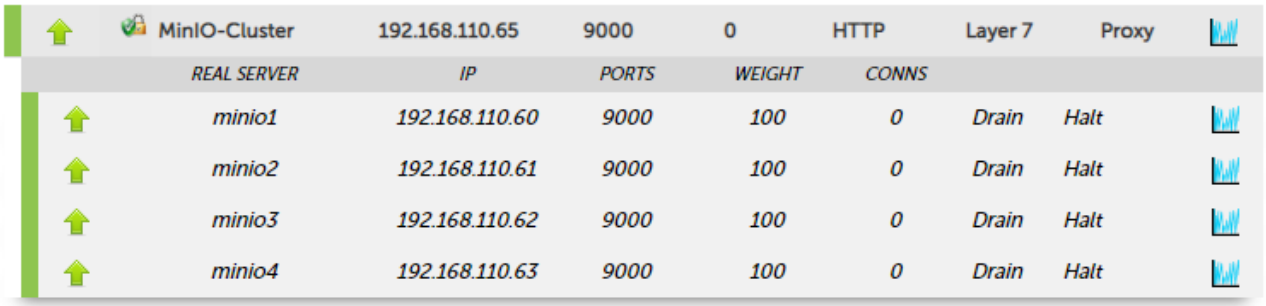
> **Note** For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

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

9.1. 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).



MinIO-Cluster	192.168.110.65	9000	0	HTTP	Layer 7	Proxy	
REAL SERVER	*IP*	*PORTS*	*WEIGHT*	*CONNS*			
minio1	*192.168.110.60*	*9000*	*100*	*0*	*Drain*	*Halt*	
minio2	*192.168.110.61*	*9000*	*100*	*0*	*Drain*	*Halt*	
minio3	*192.168.110.62*	*9000*	*100*	*0*	*Drain*	*Halt*	
minio4	*192.168.110.63*	*9000*	*100*	*0*	*Drain*	*Halt*	

9.2. 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
historic 68 MiB
```

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. 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 fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

> **Note** For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library

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.

12.1.1. 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:

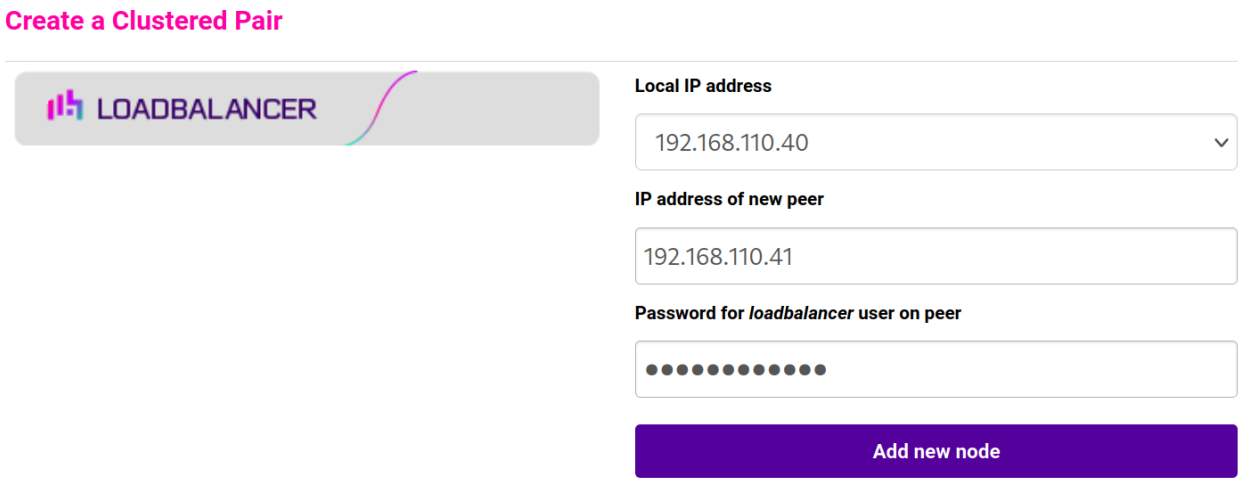
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Fallback Page	Fallback page configuration
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

> **Important** Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

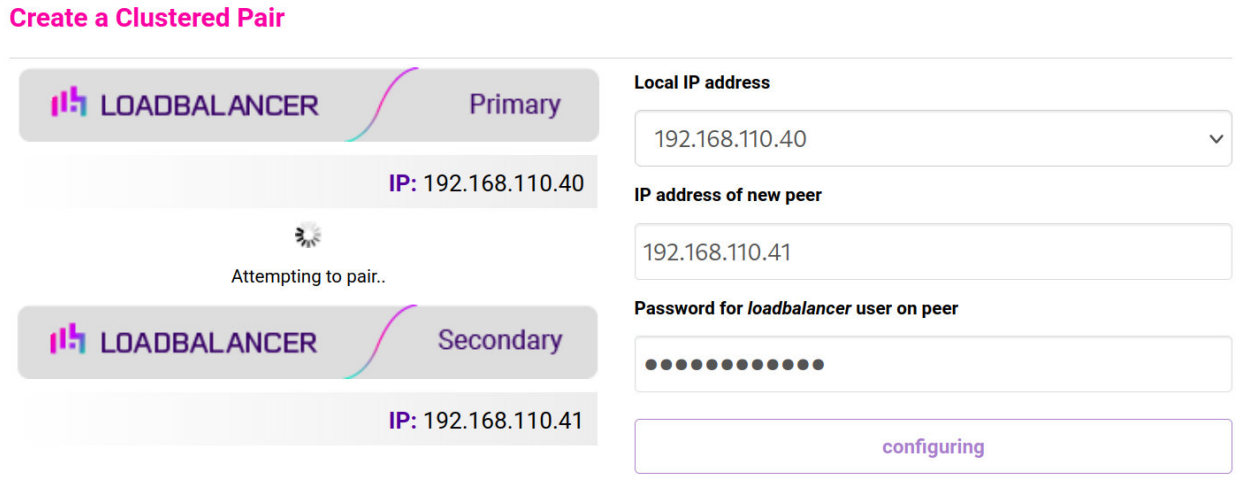
12.1.2. Configuring the HA Clustered Pair

> **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.

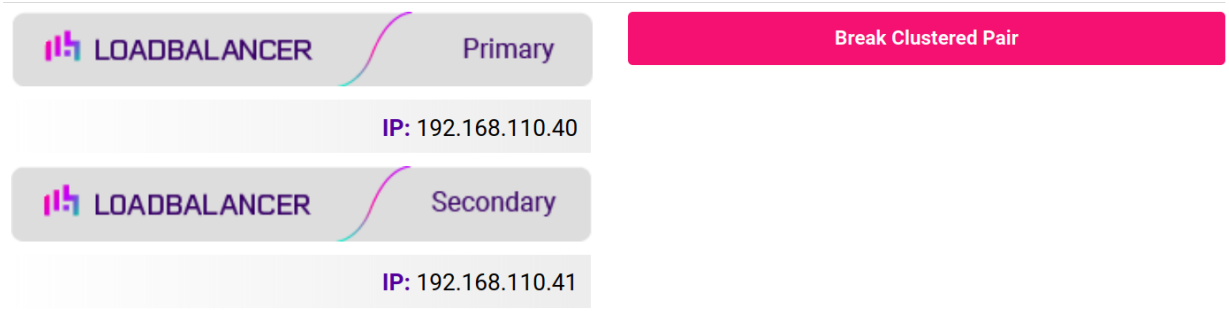
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



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.

> **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.

13. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	16 October 2019	First draft		RJC
1.0.1	29 October 2019	Expanded note on parameters to be customised in the MinIO startup command	To remind the reader to change the command to suit their environment	RJC
1.0.2	2 September 2020	New title page Updated Canadian contact details	Branding update Change to Canadian contact details	AH
1.1.0	1 December 2021	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.1.1	26 April 2022	Updated SSL related content to reflect latest software version	New software release	RJC
1.1.2	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.1.3	5 January 2023	Combined software version information into one section Added one level of section numbering Added software update instructions Added table of ports used by the appliance Reworded 'Further Documentation' section Removed references to the colour of certain UI elements	Housekeeping across all documentation	AH
1.1.4	2 February 2023	Updated screenshots	Branding update	AH
1.1.5	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.2.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

LOADBALANCER

Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: @loadbalancer.org

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.