LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing VMware App Volumes

Version 1.1.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced VMware App Volumes environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any VMware App Volumes 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 with VMware App Volumes. For full specifications of available models please refer to https://www.loadbalancer.org/products.

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. VMware App Volumes

- V2.x
- V3.x
- V4.x

4. VMware App Volumes

VMware App Volumes is a real-time application delivery system that enterprises can use to dynamically deliver and manage applications.

Applications are packaged and delivered by attaching a standard VMDK or VHD file to a virtual machine. You can centrally manage the applications with the App Volumes Manager, a Web-based interface that is integrated with Active Directory (AD) and vSphere. Administrators can assign, update, or remove applications to be delivered at the next user login without the need to modify the desktops or disrupt users while they are working.

Writable Volumes allow users to access their application data across sessions and devices.

5. Load Balancing VMware App Volumes

> **Note** It's highly recommended that you have a working VMware App Volumes environment first before implementing the load balancer.

5.1. Persistence (aka Server Affinity)

HTTP cookie persistence is required when load balancing VMware App Volumes.

5.2. Port Requirements

The following table shows the ports that are load balanced:

Port	Protocols	Use
80	TCP/HTTP	App Volumes HTTP traffic
443	TCP/HTTPS	App Volumes Secure HTTP traffic

5.3. TLS/SSL Termination

5.3.1. Server Certificates

TLS/SSL server certificates in either PFX or PEM file format can be uploaded to the Load balancer using the certificate upload. Alternatively, you can create a Certificate Signing Request (CSR) on the load balancer and send this to your CA to create a new certificate. For more information please refer to Generating a CSR on the Load Balancer.

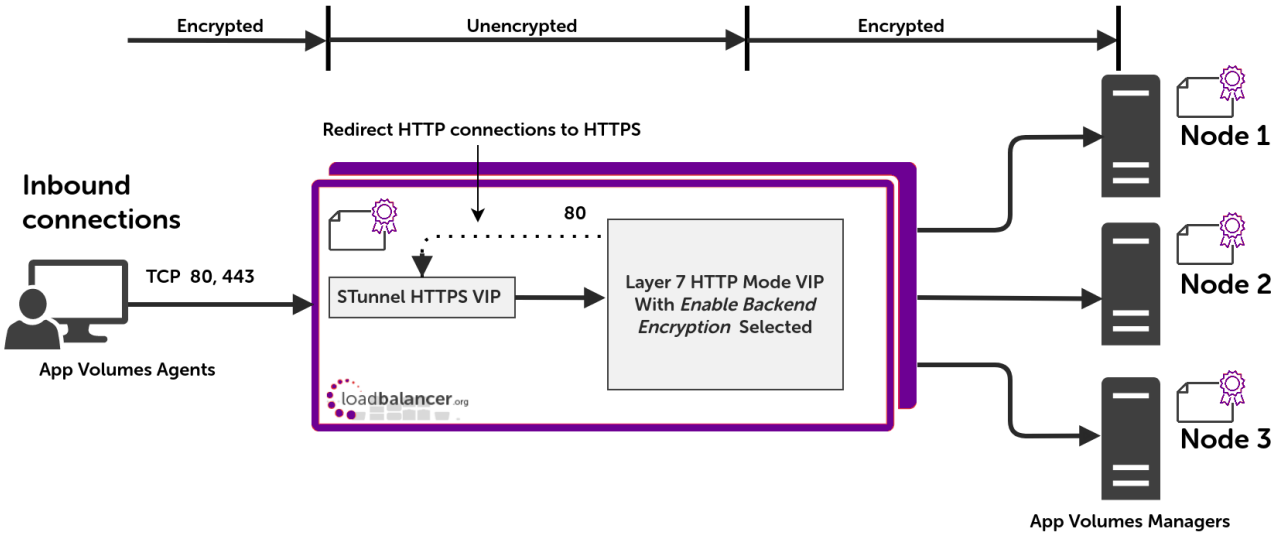
5.4. TLS/SSL Offloading with Re-encrypt to the Backend (SSL Bridging)

Terminating SSL on the load balancer is only necessary when using cookie based persistence for the primary protocol connections. Cookie based persistence is only needed when source IP address persistence cannot be used due to inline NAT/proxy devices hiding client source IP addresses. If SSL offload is used, the load balancer and the App Volumes servers ***must*** have the same certificate.

5.5. Health Checks

The load balancer is configured to check the health of each App Volumes server by periodically sending an HTTPS GET request to the location `/health_check` with the `Host` header appropriate for the FQDN in use. It will perform this HTTPS GET and expect a `200 OK` response. If it receives a response other than `200 OK` or doesn't get any response, that server will be marked as down and will not attempt to route client requests to it. It will continue to poll so that it can detect when it is available again.

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 the section Configuring HA - Adding a Secondary Appliance in the appendix for more details on configuring a clustered pair.

6.1. Virtual Service (VIP) Requirements

To provide load balancing and HA for VMWare App Volumes, a single VIP is required:

- VMWare App Volumes

7. Loadbalancer.org Appliance – the Basics

7.1. 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.

7.2. 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.

7.3. 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.

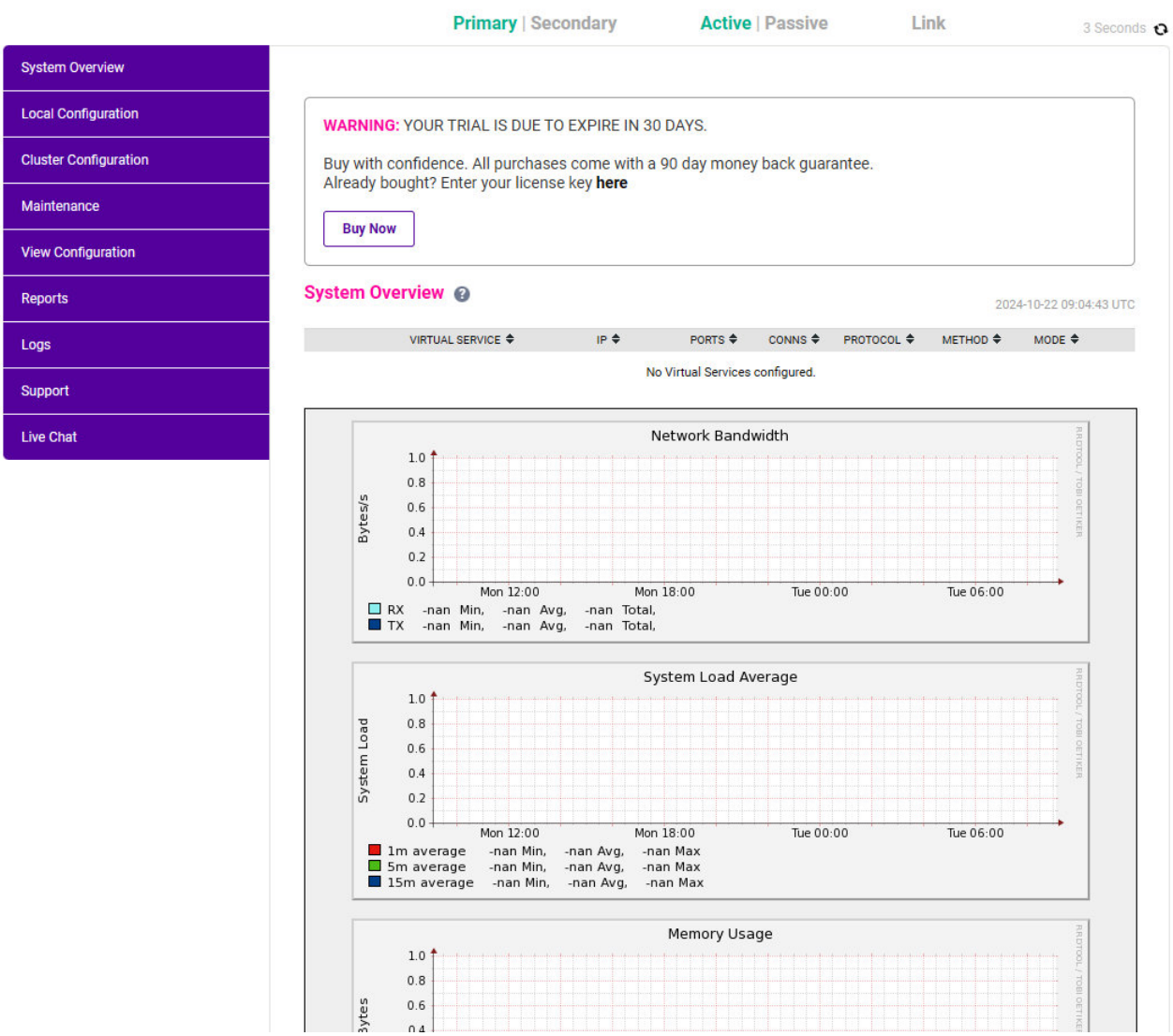
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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:



7.3.1. 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

7.4. Appliance Software Update

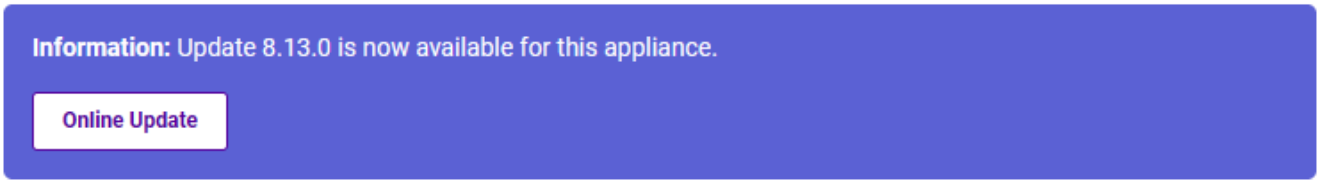
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **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.

7.4.1. Online Update

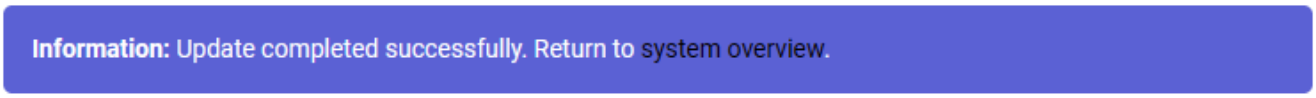
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



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.

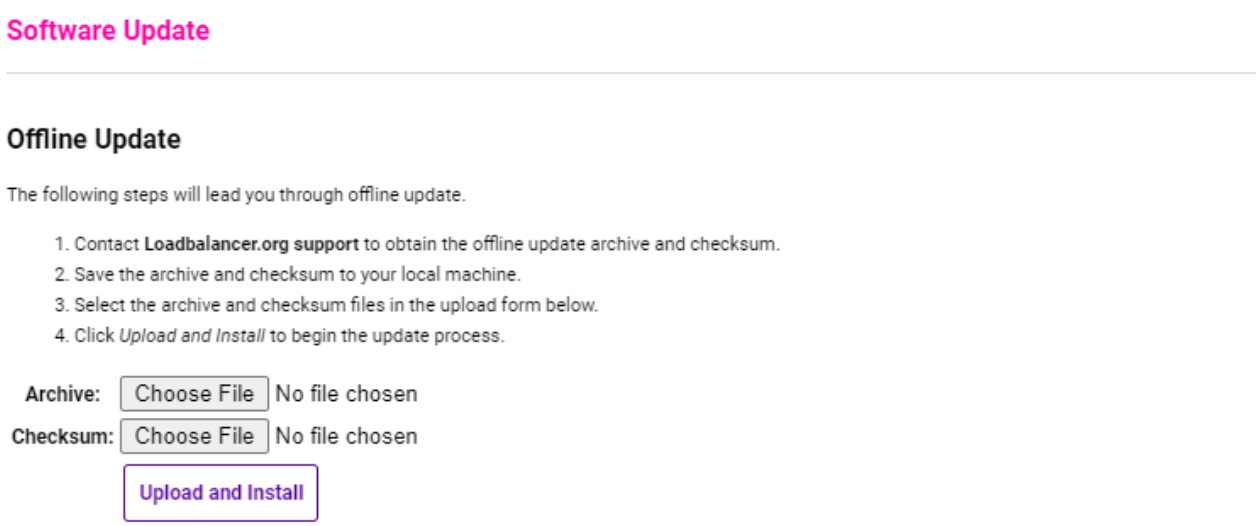
7.4.2. Offline Update

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.

7.5. 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.

7.6. HA Clustered Pair Configuration

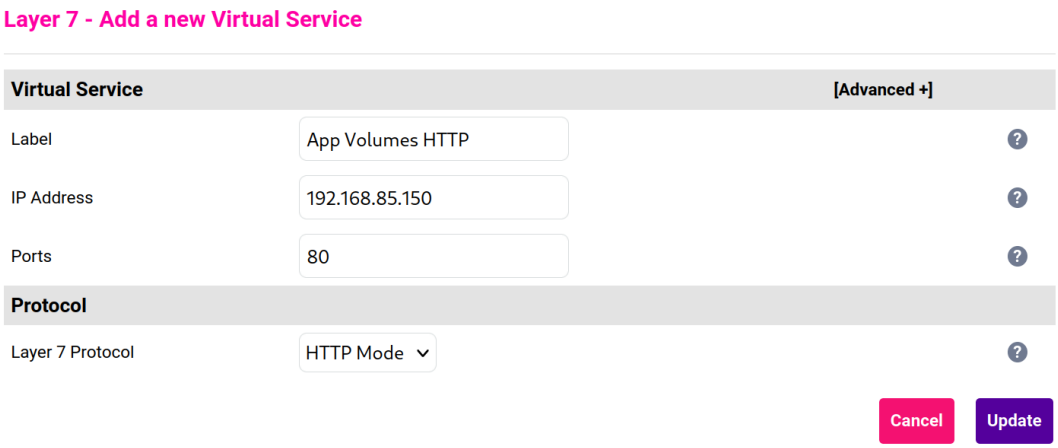
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this

guide a single unit is deployed first, adding a secondary unit is covered in the section Configuring HA - Adding a Secondary Appliance of the appendix.

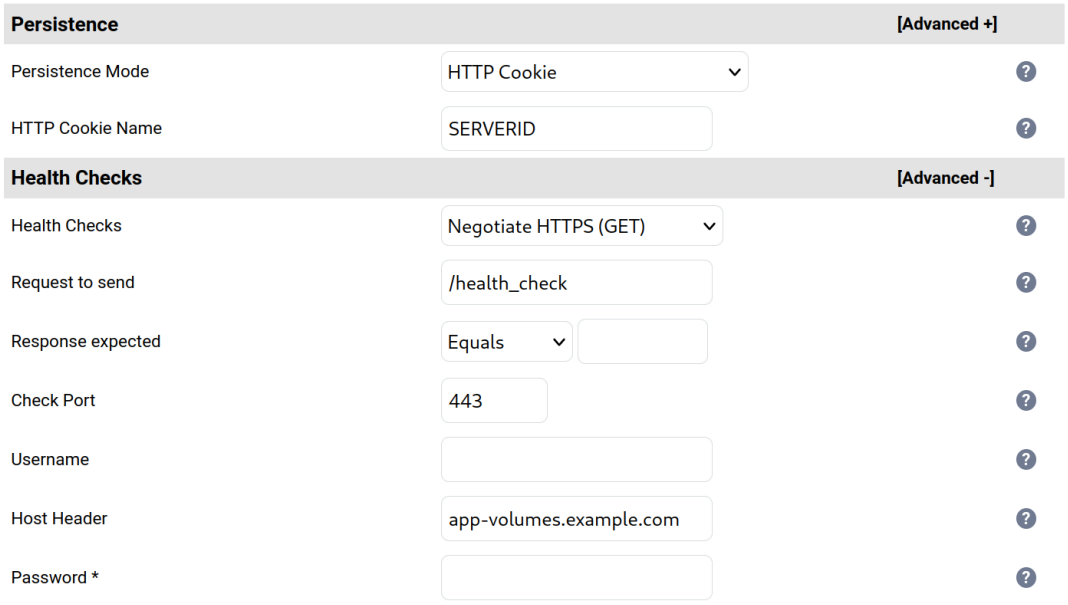
8. Appliance Configuration for VMware App Volumes

8.1. Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **App Volumes HTTP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.150**.
4. Set the *Ports* field to **80**.
5. Set the *Layer 7 Protocol* to **HTTP Mode**.
6. Click **Update** to create the virtual service.



7. Click **Modify** next to the newly created VIP.
8. Set *Persistence Mode* to **HTTP Cookie**.
9. In the *Health Checks* section click **Advanced** to expand the menu.
10. Set *Health Checks* to **Negotiate HTTPS (GET)**.
11. Set *Request to send* to **/health_check**
12. Set *Check Port* to **443**.
13. Set *Host Header* to the FQDN of the App Volumes deployment, e.g. **app-volumes.example.com**

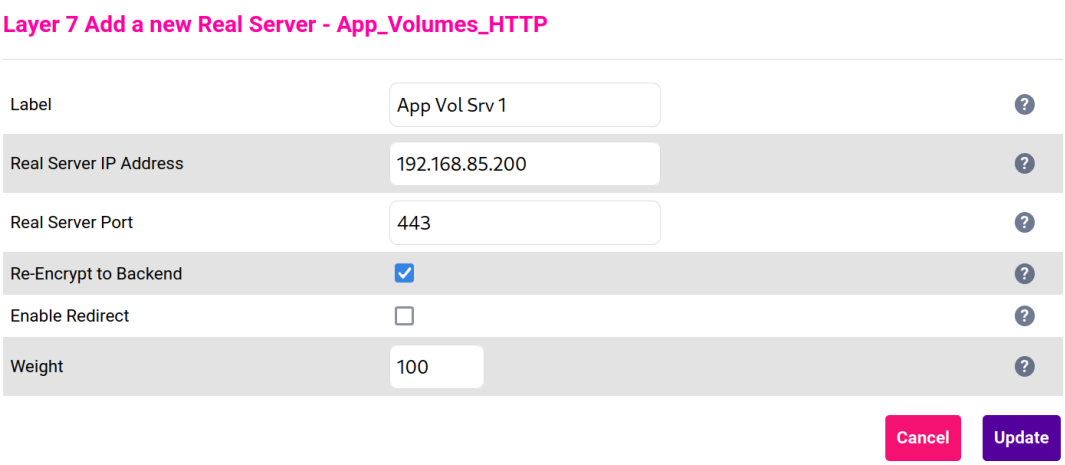


14. Under *SSL* check the **Enable Backend Encryption** checkbox.

15. Click **Update**.

8.2. 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 VIP.
2. Define the *Label* for the real server as required, e.g. **App Vol Srv 1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.200**.
4. Set the *Real Server Port* field to **443**.
5. Ensure that the **Re-Encrypt to Backend** checkbox is checked.
6. Click **Update**.
7. Repeat these steps to add additional App Volumes servers as required.



8.3. Finalizing the Configuration

To apply the new settings, HAProxy must be reloaded. This can be done using the button 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**.

9. Additional Configuration Options & Settings

9.1. TLS/SSL Termination

The load balancer can handle TLS/SSL termination in the following ways:

1. On the App Volumes servers, aka **SSL Pass-through**
2. On the load balancer, aka **SSL Offloading**
3. On the load balancer with re-encryption to the App Volumes servers, aka **SSL Bridging** (recommended)

In the "bridging" case, a TLS termination service utilizing stunnel (default and recommended) is configured on the appliance and a server certificate is uploaded and associated to the virtual service. Data is encrypted from the client to the load balancer and is also encrypted from the load balancer to the backend servers.

Notes on "SSL Bridging":

- This is similar to 'SSL Offload', the only difference is that the connection from the load balancer to the App Volumes servers is encrypted using the certificate located on the App Volumes server. This could be a self-signed certificate since no client connections are terminated here, only at the stunnel service.
- This mode can be enabled for the entire VIP and all associated App Volumes servers using the VIP option *Enable Backend Encryption* or per-App Volumes server using the *Re-Encrypt to Backend* option as detailed below.

> **Note** Performing TLS/SSL termination on the load balancer can be very CPU intensive. In most cases, for a scalable solution, terminating TLS/SSL on the App Volumes servers is the best option.

9.1.1. Backend Encryption at the Virtual Service Level (Recommended)

To enable re-encryption at the virtual service level:

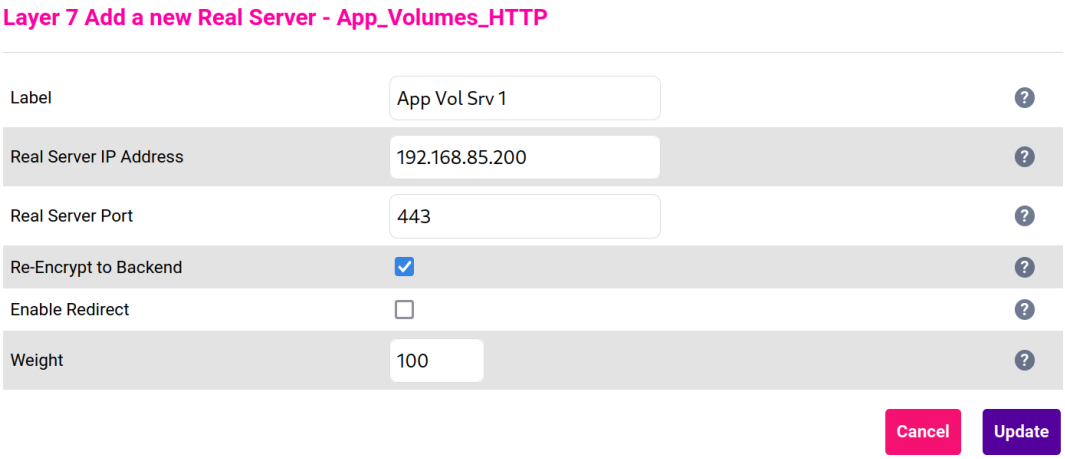
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services*.
2. Click **Modify** next to the App Volumes VIP.
3. Under *SSL* check the **Enable Backend Encryption** checkbox.

4. Click **Update**.

9.1.2. Backend Encryption at the Real Server Level

To enable re-encryption at the real server level, on a server-by-server basis:

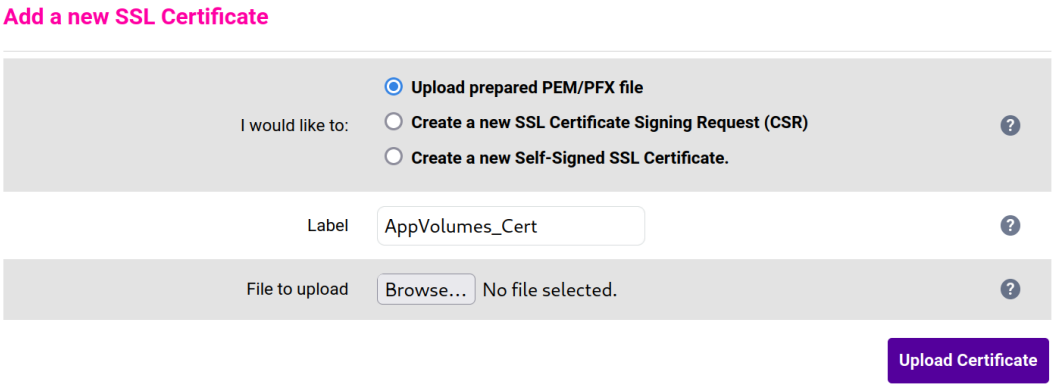
1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Real Servers*.
2. Click **Modify** next to the first App Volumes server.
3. Ensure that the **Re-Encrypt to Backend** checkbox is checked.
4. Click **Update**.
5. Repeat these steps to enable backend encryption for each App Volumes server as required.



9.1.3. Uploading a Certificate

An appropriate server certificate must be present on the load balancer for TLS/SSL termination to work. Typically, a valid certificate is uploaded to the load balancer for use. The process for doing this is as follows:

1. Using the web user interface, navigate to *Cluster Configuration > SSL Certificate* and click on **Add a new SSL Certificate**.
2. Press the **Upload prepared PEM/PFX file** radio button.
3. Define the *Label* for the certificate as required, e.g. **AppVolumes_Cert**.
4. Click on **Browse** and select the appropriate PEM or PFX style certificate.
5. If uploading a PFX certificate, enter the certificate's password in the *PFX File Password* field.
6. Click **Upload Certificate**.



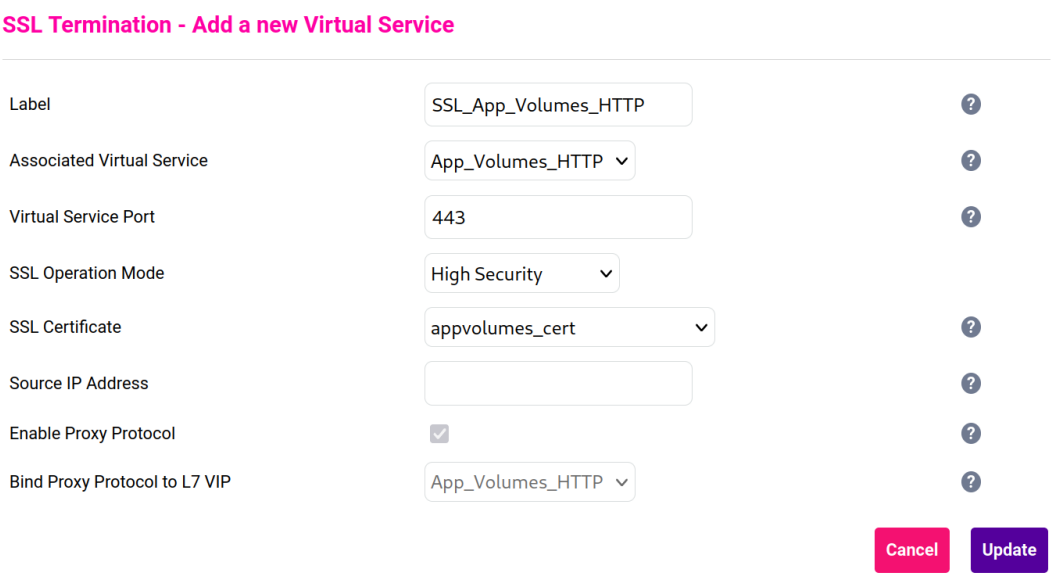
Further information on creating PEM files and converting between certificate formats can be found in our *Administration Manual*.

In the absence of a valid certificate, it is also possible to create a certificate signing request (CSR) on the load balancer. A CSR can be submitted to a certificate authority for the issuance of a certificate. Instructions on creating a CSR can be found in our *Administration Manual*.

Our *Administration Manual* can be found at: https://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf

9.1.4. Creating the TLS/SSL Termination Service (SSL Offloading)

1. Using the web user interface, navigate to *Cluster Configuration > SSL Termination* and click on **Add a new Virtual Service**.
2. From the *Associated Virtual Service* drop-down list, select the App Volumes service that was created previously.
3. Set the *Virtual Service Port* field to **443**.
4. From the *SSL Certificate* drop-down list, select the appropriate certificate.
5. Click **Update** to create the TLS/SSL termination service.



9.1.5. Creating The TLS/SSL Termination Service (SSL Bridging)

1. To configure "SSL Bridging" (TLS/SSL with re-encryption to the backend), follow the steps as per Section 9.1.1, "Backend Encryption at the Virtual Service Level (Recommended)" and enable re-encrypt to backend on the VIP.
2. Ensure that the real servers have port 443 defined with an SSL certificate installed.
3. Upload an SSL certificate to the load balancer as per the step above.
4. Create an SSL termination as per the steps above.
5. Observe that the system overview page now displays real servers with 're-encrypt to backend' padlock icons.

9.2. Enabling 'Force to HTTPS'

It is possible to force the use of TLS and disallow the use of plaintext HTTP. For security and privacy reasons, this is strongly recommended for any traffic that travels over the public internet. This is achieved by forcing all clients that connect using plaintext HTTP to reconnect using HTTPS.

1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Modify** next to the App Volumes VIP.
2. In the *Other* section click **Advanced** to expand the menu.
3. Set *Force to HTTPS* to **Yes**.
4. Click **Update**.

9.3. Finalizing the Configuration

To apply the new settings, HAProxy and stunnel must both be reloaded as follows:

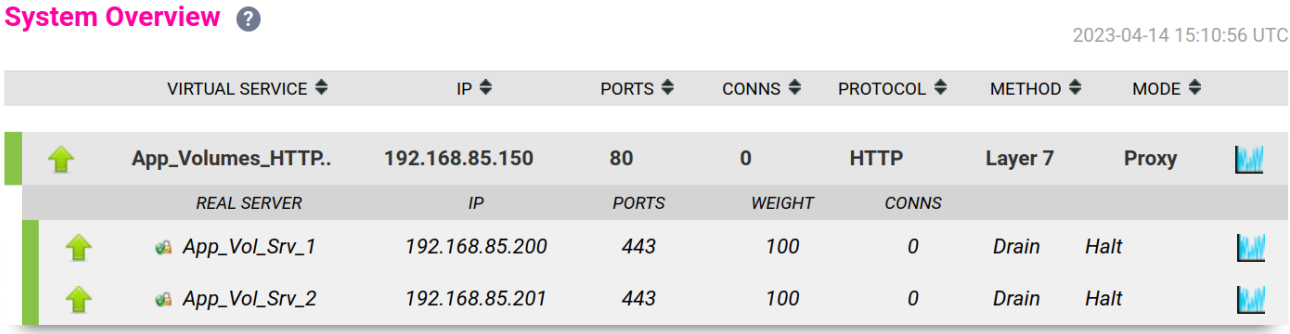
1. Using the WebUI, navigate to: *Maintenance > Restart Services* and click **Reload STunnel**
2. Using the WebUI, navigate to: *Maintenance > Restart Services* and click **Reload HAProxy**

10. Testing & Verification

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

10.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the App Volumes nodes) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows that all App Volumes nodes are healthy and available to accept connections:



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

For additional information, please refer to the Administration Manual.

13. Appendix

13.1. 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.

13.1.1. 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:

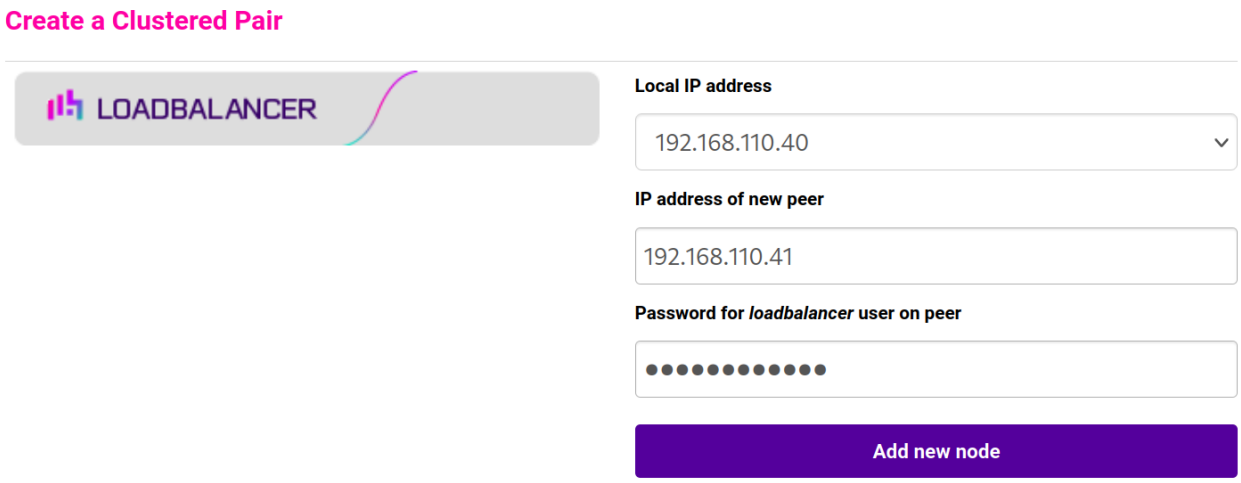
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	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.

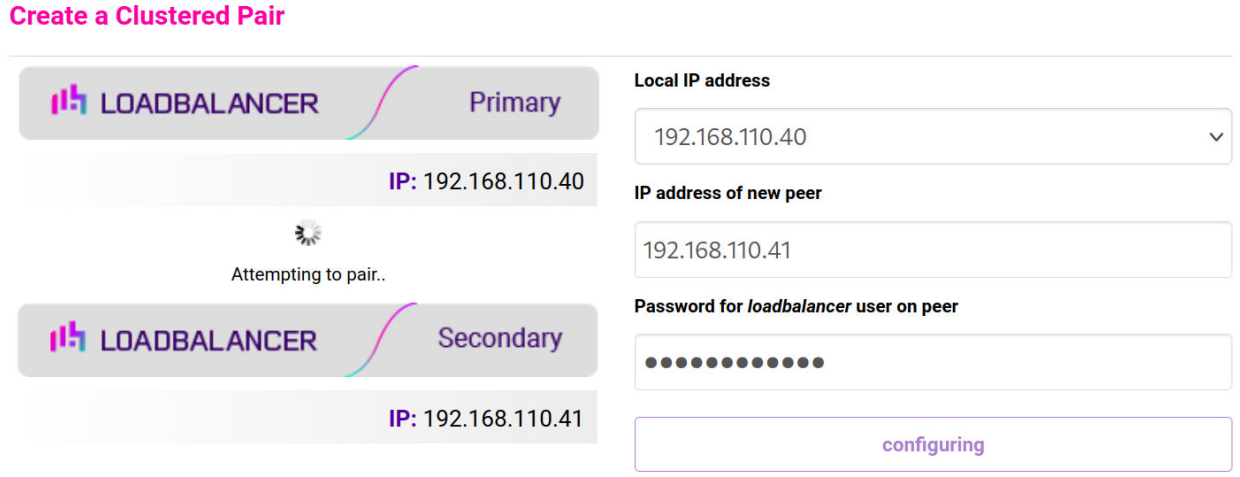
13.1.2. Configuring the HA Clustered Pair

> **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.

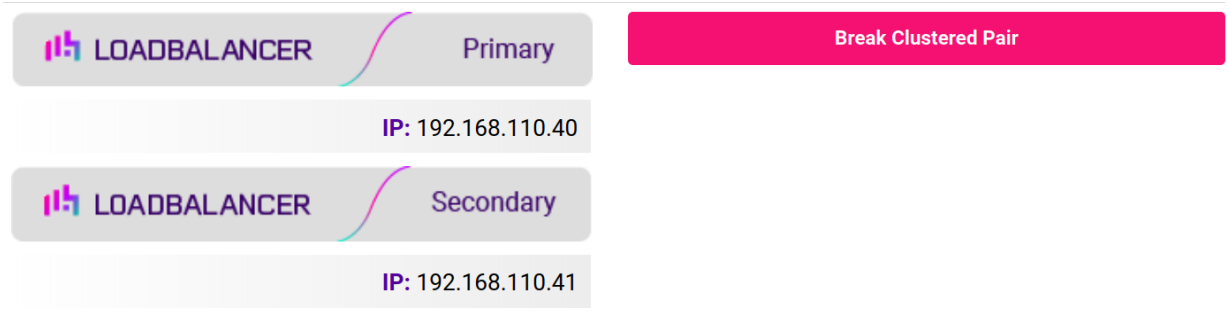
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



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.

14. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	25 September 2020	Initial creation		IBG
1.1.0	18 April 2023	Added instructions for enabling 'Force to HTTPS' Converted the document to AsciiDoc Significant updates to bring the document into line with current documentation format New document theme Modified diagram colours	'Force to HTTPS' was referenced but not previously documented step-by-step Document updates required moving it to the new documentation system 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.