Load Balancing VMware App Volumes

v1.0.0
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 relevant Administration Manual:

- v7 Administration Manual
- v8 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: http://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 details.

3. Loadbalancer.org Software Versions Supported

- v8.4.3 and later

4. VMware App Volumes Supported

- V2.x

5. 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.

6. 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.
The diagram below illustrates where the load balancers are positioned in a typical deployment.

Note: We recommend that a clustered pair of load balancers is deployed rather than a single appliance to avoid introducing a single point of failure.

**Persistence (aka Server Affinity)**

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

**Port Requirements**

The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Transport Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>HTTP traffic</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Secure HTTP traffic</td>
</tr>
</tbody>
</table>

**Virtual Service (VIP) Requirements**

To provide load balancing and HA for VMWare App Volumes, the following VIP is required:

- VMWare App Volumes

**SSL Certificates**

SSL 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) and send this to your CA to create a new certificate explained in our full administration guide [here](#).

**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.

**Load Balancer Deployment Modes**

The primary protocol is TCP/HTTPS based, Layer 7 SNAT is recommended for this deployment.

**Server Health Checks**

The load balancer is configured to check the health of each App Volumes server by periodically sending an HTTPS GET /health_check HTTP/1.1 Host: FQDN-FOR-AppVolumes Connection: Close request *(Change the FQDN-For-AppVolumes to your FQDN)*. 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.
7. Loadbalancer.org Appliance – the Basics

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.

Note: Please refer to the Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

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)

1. Browse to the following URL: https://192.168.2.21:9443/lbadmin/
   (replace with your IP address if it’s been changed)
   * Note the port number → 9443

2. Login to the WebUI:
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 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 slave unit is covered in section 2 of the Appendix on page 14.
8. Appliance Configuration for VMware App Volumes

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. Enter the following details

3. Define the Label for the virtual service as required, e.g. AppVolumes_VIP
4. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.0.160
5. Set the Ports field to 80
6. Set the Layer 7 Protocol to HTTP Mode
7. Click Update to create the virtual service
8. Click Modify next to the newly created VIP
9. Set Persistence Mode to HTTP Cookie
10. Set Health Checks to Negotiate HTTPS (GET)
11. Set Request to send to GET /health_check HTTP/1.1 Host: FQDN-FOR-AppVolumes

Note: Change the FQDN-For-AppVolumes to your FQDN

12. Click the Advanced button to expand the Health Checks menu
13. Set Check Port to 443
14. Under SSL check the Enable Backend Encryption box
15. Click **Update**

### 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. Enter the following details

![Layer 7 Add a new Real Server - AppVolumes_VIP](image)

3. Define the **Label** for the real server as required, e.g. **AppVol1**
4. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.0.41**
5. Set the **Real Server Port** to **443**
6. **Enable Re-Encrypt to Backend**
7. Click **Update**
8. Repeat these steps to add additional AppVolumes nodes as real servers as required
9. Click **Reload Haproxy** to commit the configuration

### 9. Additional Configuration Options & Settings

#### SSL Termination

SSL termination can be handled 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 this case, an SSL VIP utilizing either STunnel (default & recommended) or Pound is configured on the appliance and an SSL 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:**

- 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 or Pound VIP.
- 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: SSL termination on the load balancer can be very CPU intensive. In most cases, for a scalable solution, terminating SSL on the App Volumes servers is the best option.

To enable re-encryption at the Virtual Server level:

1. Use the WebUI menu option: *Cluster Configuration > Layer 7 – Virtual Servers > Modify*

2. Enable the option *Re-Encrypt to Backend*

3. Click *Update*

4. Now add the App Volumes servers ensuring that you specify the correct HTTPS port – typically *443*

Note: This setting only applies to App Volumes servers added after setting this option, it auto enables the Re-encrypt to Backend option (see below) for all new App Volumes servers.

To enable re-encryption at the Real Server level:

1. For each Real Server use the WebUI menu option: *Cluster Configuration > Layer 7 – Real Servers > Modify*
2. Set **Real Server Port** to **443**
3. **Enable** the option **Re-Encrypt to Backend**
4. Click **Update**
5. Repeat for your other App Volumes server(s)

**Certificates**

**Uploading A Certificate**

An appropriate 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: http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf

Creating The TLS/SSL Termination (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 AppVolumes VIP service which 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
6. Click Reload HAProxy and Reload Stunnel to commit the configuration

Creating The TLS/SSL Termination (SSL Bridging)

1. To configure SSL bridging (SSL with re-encryption to the backend) follow the steps as per section 9 of this guide 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. Next upload an SSL certificate to the load balancer as per the step above
4. Then create an SSL termination as per the steps above
5. The system overview page will display real servers with re-encrypt to backend padlock icon
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 HAProx**

10. Testing & Verification

Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIsPs (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:

![System Overview](image)

11. Technical Support

If you have any questions regarding the appliance or would like assistance designing your deployment, please don’t hesitate to contact our support team: support@loadbalancer.org.

12. Further Documentation


13. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced VMware App Volumes 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

Version 7:
Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8:
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
• 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:

![Create a Clustered Pair](image)

• Once complete, the following will be displayed:

![Create a Clustered Pair](image)

• 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>25 September 2020</td>
<td>Initial creation</td>
<td></td>
<td>IBG</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

Canada
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver,
BC, V6B 2Z4, Canada
TEL:+1 866 998 0508
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

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