Load Balancing OpenText RightFax

Version 1.2.0
# Table of Contents

1. About this Guide .................................................. 4  
2. Loadbalancer.org Appliances Supported .................. 4  
3. Software Versions Supported  
   3.1. Loadbalancer.org Appliance ......................... 4  
   3.2. OpenText RightFax ................................. 4  
4. OpenText RightFax ............................................. 4  
5. Load Balancing OpenText RightFax  
   5.1. Persistence (aka Server Affinity) ............... 4  
   5.2. Virtual Service (VIP) Requirements ........... 5  
   5.3. Port Requirements ............................... 5  
6. Deployment Concept .......................................... 5  
7. Load Balancer Deployment Methods  
   7.1. Layer 4 DR Mode .................................... 6  
   7.2. Layer 7 SNAT Mode ................................. 7  
   7.3. Our Recommendation .............................. 8  
8. Configuring OpenText RightFax for Load Balancing  
   8.1. Windows 2019 ......................................... 9  
9. Loadbalancer.org Appliance – the Basics  
   9.1. Virtual Appliance .................................... 9  
   9.2. Initial Network Configuration ..................... 9  
   9.3. Accessing the WebUI  
       Main Menu Options .................................. 10  
   9.4. Appliance Software Update  
       Determining the Current Software Version ........ 12  
       Checking for Updates using Online Update ....... 12  
       Using Offline Update ................................ 12  
   9.5. Ports Used by the Appliance ....................... 13  
   9.6. HA Clustered Pair Configuration ................. 14  
10. Appliance Configuration for OpenText RightFax – Using Layer 4 DR Mode  
   10.1. Configuring VIP 1 - Client Access (HTTP)  
       Configuring the Virtual Service (VIP) ........... 14  
       Defining the Real Servers (RIPs) ................. 15  
   10.2. Configuring VIP 2 - Client Access (HTTPS)  
       Configuring the Virtual Service (VIP) ........... 15  
       Defining the Real Servers (RIPs) ................. 16  
   10.3. Configuring VIP 3 - Network File Storage (SMB/LPD)  
       Configuring the Virtual Service (VIP) ........... 17  
       Defining the Real Servers (RIPs) ................. 17  
   10.4. Configuring VIP 4 - Client Access (Server Module)  
       Configuring the Virtual Service (VIP) ........... 18  
       Defining the Real Servers (RIPs) ................. 18  
   10.5. Configuring VIP 5 - Licensing  
       Configuring the Virtual Service (VIP) ........... 19  
       Defining the Real Servers (RIPs) ................. 19  
11. Appliance Configuration for OpenText RightFax – Using Layer 7 SNAT Mode  
   11.1. Configuring VIP 1 - Client Access (HTTP)  
       Configuring the Virtual Service (VIP) ........... 21  
       Defining the Real Servers (RIPs) ................. 21
1. About this Guide

This guide details the steps required to configure a load balanced OpenText RightFax environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any OpenText RightFax 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 OpenText RightFax. 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. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.5.3 and later

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.

3.2. OpenText RightFax

- Versions 20.2.0.0 to 20.2.2.277

4. OpenText RightFax

Installed on a local area network (LAN), OpenText™ RightFax™ lets users, applications, and systems connected to the network send and receive paperless, digital faxes. The enterprise fax server software connects to onsite analog or digital telephony, voice-over-IP telephony, or the cloud to transmit the fax securely. Integrated with email for users and back-end systems for application faxing, RightFax significantly reduces the total cost of faxing across an enterprise.

5. Load Balancing OpenText RightFax

5.1. Persistence (aka Server Affinity)

- It’s highly recommended that you have a working OpenText RightFax environment first before implementing the load balancer.
OpenText RightFax does not require session affinity at the load balancing layer.

5.2. Virtual Service (VIP) Requirements
To provide load balancing and HA for OpenText RightFax, the following VIPs are required:

- Client Access (HTTP)
- Client Access (HTTPS)
- Network File Storage (SMB/LPD)
- Server Module Client Access
- Licensing

5.3. Port Requirements
The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Ports</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP/HTTP</td>
<td>Provides page rendering services, auditing, reporting, HTTP transfer fallback capability for clients that cannot establish OpenText Fuel connection with the server</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>Provides page rendering services, auditing, reporting, HTTPS transfer fallback capability for clients that cannot establish OpenText Fuel connection with the server</td>
</tr>
<tr>
<td>445/515</td>
<td>TCP/SMB, TCP/LPD</td>
<td>Network accessible file storage for Secure MFT to store the file assets</td>
</tr>
<tr>
<td>10520-10522, 10062, 34001, 34988</td>
<td>TCP</td>
<td>Server Module (client access)</td>
</tr>
<tr>
<td>36363</td>
<td>TCP</td>
<td>Licensing</td>
</tr>
</tbody>
</table>

6. Deployment Concept
7. Load Balancer Deployment Methods

The load balancer can be deployed in 4 fundamental ways: **Layer 4 DR mode**, **Layer 4 NAT mode**, **Layer 4 SNAT mode**, and **Layer 7 SNAT mode**.

For OpenText RightFax, using layer 4 DR mode is recommended. It is also possible to use layer 7 SNAT mode, however the performance of this set up is not as great as layer 4 DR mode. These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode please refer to the section **Appliance Configuration for OpenText RightFax – Using Layer 4 DR Mode**, and for configuring using layer 7 SNAT mode refer to the section **Appliance Configuration for OpenText RightFax – Using Layer 7 SNAT Mode**.

7.1. Layer 4 DR Mode

One-arm direct routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.

© Copyright Loadbalancer.org • Documentation • Load Balancing OpenText RightFax
DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.

When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Server's own IP address and the VIP.

The Real Servers should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as **Solving the ARP problem**. For more information please refer to **DR Mode Considerations**.

On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP.

The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work.

The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet.

Port translation is not possible with DR mode, e.g. **VIP:80 → RIP:8080** is not supported.

DR mode is transparent, i.e. the Real Server will see the source IP address of the client.

### 7.2. Layer 7 SNAT Mode

Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer and HAProxy generates a new corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.
Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.

Layer 7 SNAT mode is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancer’s own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address). This can be configured per layer 7 VIP. If required, the load balancer can be configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client’s source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to Transparency at Layer 7.

Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration. For two-arm deployments, eth0 is normally used for the internal network and eth1 is used for the external network although this is not mandatory.

Requires no mode-specific configuration changes to the load balanced Real Servers.

Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.

You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

7.3. Our Recommendation

Where possible, we recommend that Layer 4 Direct Routing (DR) mode is used. This mode offers the best possible performance since replies go directly from the Real Servers to the client, not via the load balancer. It’s also relatively simple to implement. Ultimately, the final choice does depend on your specific requirements and infrastructure.

If DR mode cannot be used, for example if the real servers are located in remote routed networks, then SNAT mode is recommended.

If the load balancer is deployed in AWS, Azure, or GCP, layer 7 SNAT mode must be used as layer 4 direct routing...
is not currently possible on these platforms.

8. Configuring OpenText RightFax for Load Balancing

To enable the RightFax servers to be accessed via a shared name (e.g. `faxserver-vip`), the following steps must be completed:

8.1. Windows 2019

Host entries must be added to the local hosts file on each RightFax server. For example, if you have 2 RightFax servers: 192.168.100.20 and 192.168.100.21, add the following entries to the hosts files:

**On the 192.168.100.20 server**
```
192.168.100.20 faxserver-vip 192.168.100.20 faxserver-vip.domain.com
```

**On the 192.168.100.21 server**
```
192.168.100.21 faxserver-vip 192.168.100.21 faxserver-vip.domain.com
```

where `faxserver-vip` is the DNS name clients use to access the load balanced RightFax servers.

9. Loadbalancer.org Appliance – the Basics

9.1. 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](#).

<table>
<thead>
<tr>
<th>Note</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>Please refer to <a href="#">Virtual Appliance Installation</a> and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.</td>
</tr>
<tr>
<td>Note</td>
<td>The VA has 4 network adapters. For VMware only the first adapter (<code>eth0</code>) 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.</td>
</tr>
</tbody>
</table>

9.2. Initial Network Configuration

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

| Important | Be sure to set a secure password for the load balancer, when prompted during the setup routine. |
9.3. Accessing the 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.

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

A number of compatibility issues have been found with various versions of Microsoft Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

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


   You'll receive a warning about the WebUI's 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.

2. Log in to the WebUI using the following credentials:

   **Username**: loadbalancer
   **Password**: <configured-during-network-setup-wizard>

   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.

**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
- **Support** - Create a support download, contact the support team & access useful links
9.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

The software version is displayed at the bottom of the WebUI as shown in the example below:

Checking for Updates using Online Update

1. Using the WebUI, navigate to: Maintenance > Software Update.
2. Select Online Update.
3. If the latest version is already installed, a message similar to the following will be displayed:

   Information: Version v8.9.0 is the current release. No updates are available

4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click Online Update to start the update process.

   Note: Do not navigate away whilst the update is ongoing, this may cause the update to fail.

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

   Information: Update completed successfully.

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

Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.
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:

**Software Update**

**Offline Update**

The following steps will lead you through offline update.

1. Contact support@loadbalancer.org to obtain the offline update archive and checksum.
2. Save the archive and checksum to your local machine.
3. Select the archive and checksum files in the upload form below.
4. Click Upload and Install to begin the update process.

- **Archive**: Choose File
- **Checksum**: Choose File

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.

### 9.5. Ports Used by the Appliance

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>53</td>
<td>DNS</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>123</td>
<td>NTP</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>161</td>
<td>SNMP</td>
</tr>
<tr>
<td>UDP</td>
<td>6694</td>
<td>Heartbeat between Primary &amp; Secondary appliances in HA mode</td>
</tr>
<tr>
<td>TCP</td>
<td>7778</td>
<td>HAPProxy persistence table replication</td>
</tr>
<tr>
<td>TCP</td>
<td>9080</td>
<td>WebUI - HTTP (disabled by default)</td>
</tr>
<tr>
<td>TCP</td>
<td>9081</td>
<td>Nginx fallback page</td>
</tr>
<tr>
<td>TCP</td>
<td>9443</td>
<td>WebUI - HTTPS</td>
</tr>
</tbody>
</table>
9.6. 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.

10. Appliance Configuration for OpenText RightFax – Using Layer 4 DR Mode

10.1. Configuring VIP 1 - Client Access (HTTP)

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service.
2. Define the Label for the virtual service as required, e.g. access_http.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.140.
4. Set the Ports field to 80.
5. Leave the Protocol set to TCP.
7. Click Update to create the virtual service.

8. Click Modify next to the newly created VIP.
9. Ensure that the Persistence Enable checkbox is not checked.
10. Click Update.
Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – 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. rightfax_server_1.
3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.190.
4. Click Update.
5. Repeat these steps to add additional RightFax servers as required.

10.2. Configuring VIP 2 - Client Access (HTTPS)

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service.
2. Define the Label for the virtual service as required, e.g. access_https.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.140.
4. Set the Ports field to 443.
5. Leave the Protocol set to TCP.
7. Click Update to create the virtual service.
8. Click **Modify** next to the newly created VIP.

9. Ensure that the **Persistence Enable** checkbox is not checked.

10. Click **Update**.

**Defining the Real Servers (RIPs)**

1. Using the web user interface, navigate to **Cluster Configuration > Layer 4 – 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. `rightfax_server_1`.

3. Set the **Real Server IP Address** field to the required IP address, e.g. `192.168.85.190`.

4. Click **Update**.

5. Repeat these steps to add additional RightFax servers as required.
10.3. Configuring VIP 3 - Network File Storage (SMB/LPD)

Configuring the Virtual Service (VIP)
1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service.
2. Define the Label for the virtual service as required, e.g. net_filestorage.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.140.
4. Set the Ports field to 445,515.
5. Leave the Protocol set to TCP.
7. Click Update to create the virtual service.

Layer 4 - Add a new Virtual Service

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>net_filestorage</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.85.140</td>
</tr>
<tr>
<td>Ports</td>
<td>445,515</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
</tbody>
</table>

8. Click Modify next to the newly created VIP.
9. Ensure that the Persistence Enable checkbox is not checked.
10. Click Update.

Defining the Real Servers (RIPs)
1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – 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. rightfax_server_1.
3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.190.
4. Click Update.
5. Repeat these steps to add additional RightFax servers as required.
10.4. Configuring VIP 4 - Client Access (Server Module)

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to **Cluster Configuration > Layer 4 – Virtual Services** and click on **Add a new Virtual Service**.

2. Define the **Label** for the virtual service as required, e.g. `access_srv_mod`.

3. Set the **Virtual Service IP Address** field to the required IP address, e.g. `192.168.85.140`.

4. Set the **Ports** field to `10520-10522,10062,34001,34988`.

5. Leave the **Protocol** set to **TCP**.

6. Leave the **Forwarding Method** set to **Direct Routing**.

7. Click **Update** to create the virtual service.

8. Click **Modify** next to the newly created VIP.
9. Ensure that the Persistence Enable checkbox is not checked.

10. Click Update.

Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – 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. rightfax_server_1.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.190.

4. Click Update.

5. Repeat these steps to add additional RightFax servers as required.

<table>
<thead>
<tr>
<th>Layer 4 Add a new Real Server - access_srv_mod</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
</tr>
<tr>
<td><strong>Real Server IP Address</strong></td>
</tr>
<tr>
<td><strong>Weight</strong></td>
</tr>
<tr>
<td><strong>Minimum Connections</strong></td>
</tr>
<tr>
<td><strong>Maximum Connections</strong></td>
</tr>
</tbody>
</table>

10.5. Configuring VIP 5 - Licensing

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service.

2. Define the Label for the virtual service as required, e.g. licensing.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.140.

4. Set the Ports field to 36363.

5. Leave the Protocol set to TCP.


7. Click Update to create the virtual service.
8. Click Modify next to the newly created VIP.

9. Ensure that the Persistence Enable checkbox is not checked.

10. Click Update.

Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – 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. rightfax_server_1.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.190.

4. Click Update.

5. Repeat these steps to add additional RightFax servers as required.
11. Appliance Configuration for OpenText RightFax – Using Layer 7 SNAT Mode

11.1. Configuring VIP 1 - Client Access (HTTP)

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. access_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 TCP Mode.
6. Click Update to create the virtual service.

![Layer 7 - Add a new Virtual Service](image)

7. Click Modify next to the newly created VIP.
8. Set Persistence Mode to None.
9. 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. Define the Label for the real server as required, e.g. rightfax_server_1.
3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.190.
4. Click Update.
5. Repeat these steps to add additional RightFax servers as required.
11.2. Configuring VIP 2 - Client Access (HTTPS)

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. access_https.
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 443.
5. Set the Layer 7 Protocol to TCP Mode.
6. Click Update to create the virtual service.
7. Click Modify next to the newly created VIP.
8. Set Persistence Mode to None.
9. 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. Define the Label for the real server as required, e.g. rightfax_server_1.
3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.190.
4. Click Update.
5. Repeat these steps to add additional RightFax servers as required.

Layer 7 Add a new Real Server - access_https-1

<table>
<thead>
<tr>
<th>Label</th>
<th>rightfax_server_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.85.190</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td>[ ]</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

11.3. Configuring VIP 3 - Network File Storage (SMB/LPD)

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. net_filestorage.
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 445,515.
5. Set the Layer 7 Protocol to TCP Mode.
6. Click Update to create the virtual service.
Click Modify next to the newly created VIP.

Set Persistence Mode to None.

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. Define the Label for the real server as required, e.g. rightfax_server_1.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.190.

4. Click Update.

5. Repeat these steps to add additional RightFax servers as required.

**11.4. Configuring VIP 4 - Client Access (Server Module)**

**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. access_srv_mod.

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 10520-10522,10062,34001,34988.

5. Set the Layer 7 Protocol to TCP Mode.

6. Click Update to create the virtual service.

### Layer 7 - Add a new Virtual Service

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th>[Advanced +]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>access_srv_mod</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.85.150</td>
</tr>
<tr>
<td>Ports</td>
<td>20-10522,10062,34001,34988</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

7. Click Modify next to the newly created VIP.

8. Set Persistence Mode to None.

9. 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. Define the Label for the real server as required, e.g. rightfax_server_1.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.190.

4. Click Update.

5. Repeat these steps to add additional RightFax servers as required.
11.5. Configuring VIP 5 - Licensing

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. licensing.
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 36363.
5. Set the Layer 7 Protocol to TCP Mode.
6. Click Update to create the virtual service.

7. Click Modify next to the newly created VIP.
8. Set Persistence Mode to None.
9. 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. Define the **Label** for the real server as required, e.g. `rightfax_server_1`.

3. Set the **Real Server IP Address** field to the required IP address, e.g. `192.168.85.190`.

4. Click **Update**.

5. Repeat these steps to add additional RightFax servers as required.

---

### 11.6. 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**.

---

### 12. Testing & Verification

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

#### 12.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the RightFax servers) and shows the state/health of each server as well as the state of the cluster as a whole.

The example below shows a **layer 4 DR mode** configuration load balancing a pair of RightFax servers, where both servers are healthy and available to accept connections:
The example below shows a **layer 7 SNAT mode** configuration load balancing a pair of RightFax servers, where both servers are healthy and available to accept connections:
### 13. 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.

### 14. Further Documentation

For additional information, please refer to the Administration Manual.
15. Appendix

15.1. 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 configured first and 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>
Make sure that if these settings/updates have been configured on the Primary appliance, they're also configured on the Secondary appliance.

Adding a Secondary Appliance - Create an HA Clustered Pair

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](#).
## 16. 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>26 August 2021</td>
<td>Initial version</td>
<td></td>
<td>NH, AH</td>
</tr>
</tbody>
</table>
| 1.1.0   | 14 January 2022 | Add additional required ports for the "server module access" VIP  
Add additional required VIP for "licensing"  
Update diagrams and screenshots to reflect new ports and VIPs | Requested technical changes from OpenText              | NH, AH     |
| 1.1.1   | 28 September 2022 | Updated layer 7 VIP and RIP creation screenshots | Reflect changes in the web user interface              | AH         |
| 1.1.2   | 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 | Housekeeping across all documentation                   | AH         |
| 1.1.3   | 2 February 2023  | Updated screenshots                                                                                                                    | Branding update                                        | AH         |
| 1.1.4   | 7 March 2023     | Added the section "Finalizing the Configuration" to ensure HAProxy is explicitly reloaded  
Removed conclusion section | Provided clarity for reloading HAProxy post-configuration  
Updates across all documentation | AH         |
| 1.2.0   | 24 March 2023    | New document theme  
Modified diagram colours                                                                                                               | Branding update                                        | AH         |
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.