

Load Balancing OpenText RightFax

Version 1.2.1



Table of Contents

1. About this Guide	4
2. Loadbalancer.org Appliances Supported	4
3. Software Versions Supported	4
3.1. Loadbalancer.org Appliance	4
3.2. OpenText RightFax	4
4. OpenText RightFax	4
5. Load Balancing OpenText RightFax	4
5.1. Persistence (aka Server Affinity)	5
5.2. Virtual Service (VIP) Requirements	5
5.3. Port Requirements	5
6. Deployment Concept	5
7. Load Balancer Deployment Methods	6
7.1. Layer 4 DR Mode	6
7.2. Layer 7 SNAT Mode	7
7.3. Our Recommendation	8
8. Loadbalancer.org Appliance – the Basics	9
8.1. Virtual Appliance	9
8.2. Initial Network Configuration	9
8.3. Accessing the Appliance WebUI	9
8.3.1. Main Menu Options	11
8.4. Appliance Software Update	11
8.4.1. Online Update	11
8.4.2. Offline Update	12
8.5. Ports Used by the Appliance	12
8.6. HA Clustered Pair Configuration	13
9. Loadbalancing OpenText RightFax – Using Layer 4 DR Mode	13
9.1. Prepare the OpenText RightFax Servers for Load Balancing	13
9.1.1. Solve the ARP Problem	13
9.1.2. Enable Print and Document Server Load Balancing	18
9.2. Configure the Virtual Services	21
9.2.1. VIP 1 - Client Access (HTTP)	21
9.2.2. VIP 2 - Client Access (HTTPS)	22
9.2.3. VIP 3 - Network File Storage (SMB/LPD)	24
9.2.4. VIP 4 - Client Access (Server Module)	25
9.2.5. VIP 5 - Licensing	26
10. Loadbalancing OpenText RightFax – Using Layer 7 SNAT Mode	28
10.1. Prepare the OpenText RightFax Servers for Load Balancing	28
10.1.1. Enable Print and Document Server Load Balancing	28
10.2. Configure the Virtual Services	30
10.2.1. VIP 1 - Client Access (HTTP)	30
10.2.2. VIP 2 - Client Access (HTTPS)	32
10.2.3. VIP 3 - Network File Storage (SMB/LPD)	33
10.2.4. VIP 4 - Client Access (Server Module)	34
10.2.5. VIP 5 - Licensing	36
10.3. Finalizing the Configuration	37
11. Testing & Verification	37
11.1. Using System Overview	37
12. Technical Support	38

13. Further Documentation 38

14. Appendix 39

 14.1. Configuring HA - Adding a Secondary Appliance 39

 14.1.1. Non-Replicated Settings 39

 14.1.2. Configuring the HA Clustered Pair 40

15. Document Revision History 42

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/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. OpenText RightFax

- Versions 20.2.0.0 and later

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

Note

It's highly recommended that you have a working OpenText RightFax environment first before implementing the load balancer.



5.1. Persistence (aka Server Affinity)

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

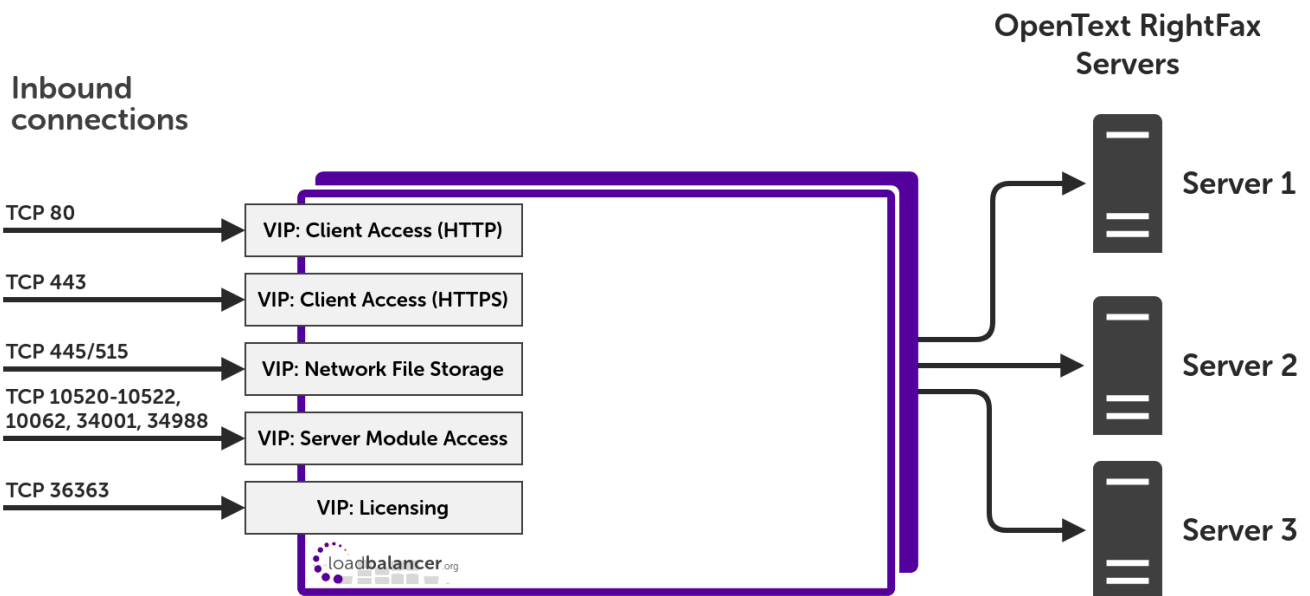
5.3. Port Requirements

The following table shows the ports that are load balanced:

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

6. Deployment Concept





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.

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*.

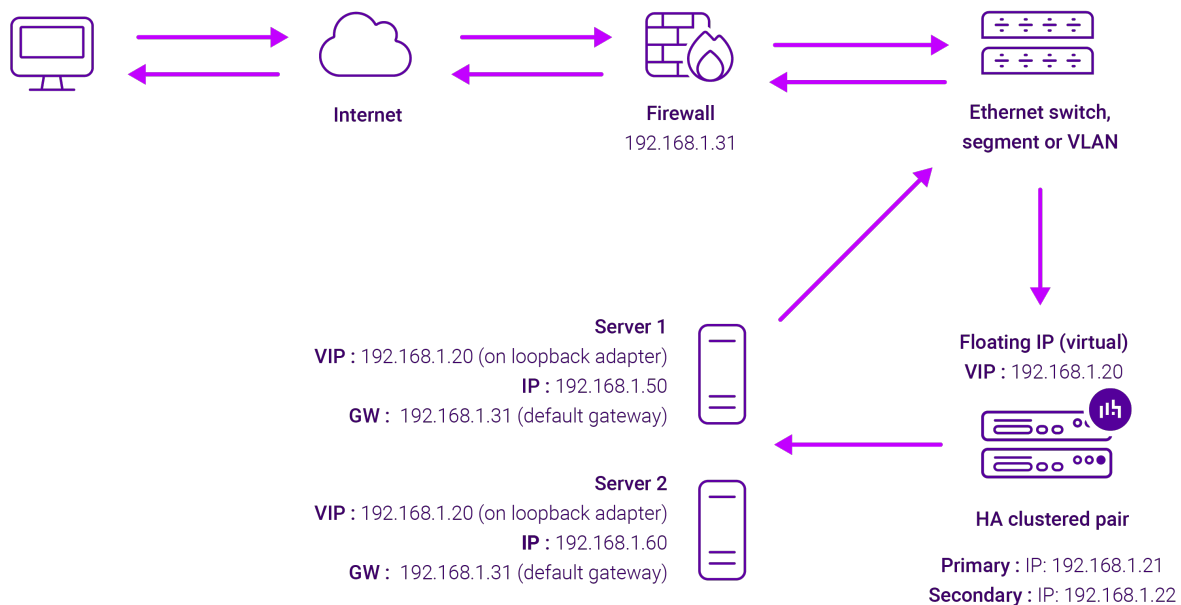
For OpenText RightFax, using layer 4 DR mode is recommended. It's also possible to use layer 7 SNAT mode, however this mode is not as fast as layer 4 DR mode. These modes are described below and are used for the configurations presented in this guide.

7.1. Layer 4 DR Mode

Layer 4 DR (Direct Routing) mode is a very high performance solution that requires little change to your existing infrastructure. The image below shows an example network diagram for this mode.

Note

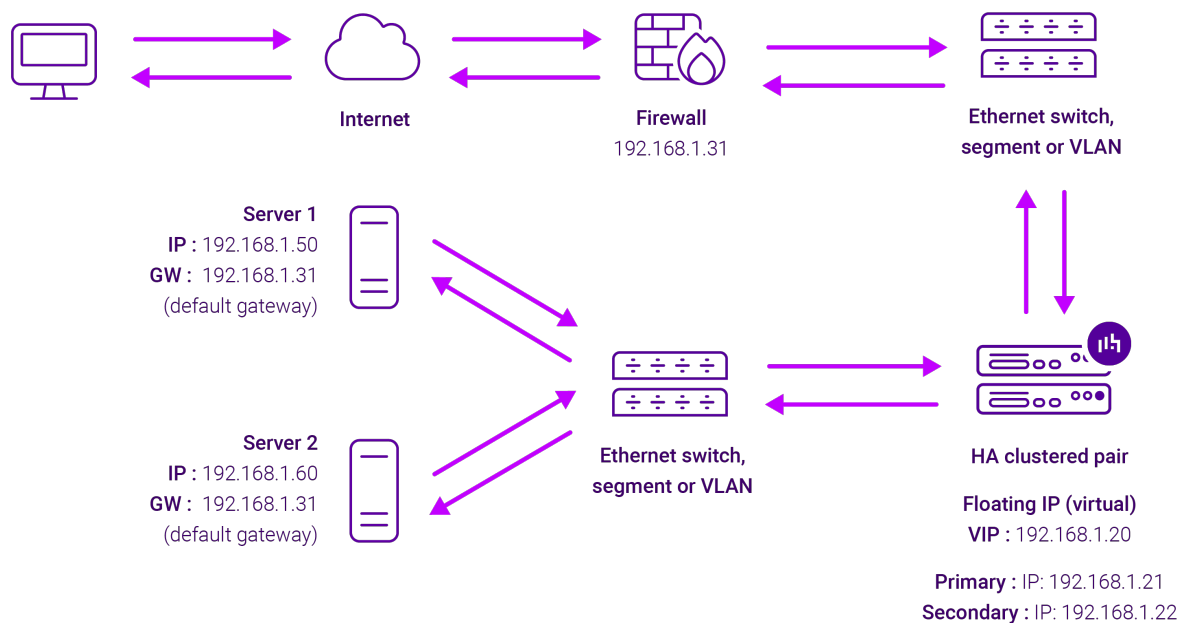
Kemp, Brocade, Barracuda & A10 Networks call this *Direct Server Return* and F5 call it *nPath*.



- 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 each Real Server (and the load balanced application) must respond to both the Real Server's own IP address and the VIP.
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Server 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 mode for HTTP and much faster for other applications such as Remote Desktop Services, streaming media and FTP.
- The load balancer must have an interface in the same subnet as the Real Servers to ensure layer 2 connectivity which is required for DR mode to operate.
- 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. The image below shows an example network diagram for this mode.



- Because layer 7 SNAT mode is a full proxy, Real Servers in the cluster can be on any accessible network 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, **eth1** is typically used for client side connections and **eth0** is used for Real Server connections, although this is not mandatory since any interface can be used for any purpose.
- 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. Loadbalancer.org Appliance – the Basics

8.1. 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.

8.2. 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.

8.3. 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](#).

- Log in to the WebUI using the following credentials:

Username: loadbalancer

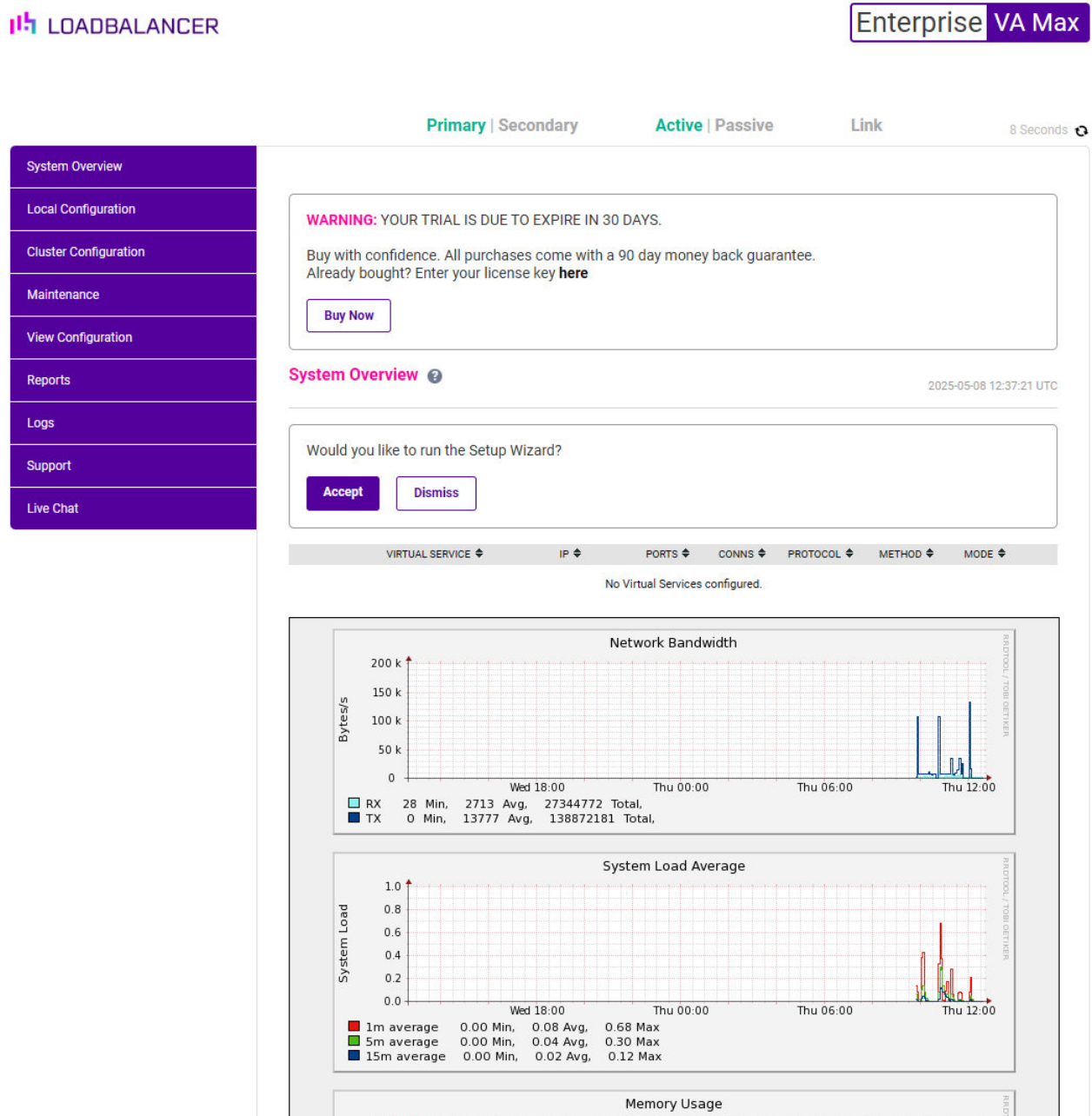
Password: <configured-during-network-setup-wizard>



Note

To change the password, use the WebUI menu option: **Maintenance > Passwords**.

Once logged in, the WebUI will be displayed as shown below:



- 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.

8.3.1. 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

8.4. 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.

8.4.1. 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:

Information: Update 8.13.2 is now available for this appliance.

Online Update

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:



Information: Update completed successfully. Return to system overview.

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

8.4.2. 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:

Software Update

Offline Update

The following steps will lead you through offline update.

1. Contact **Loadbalancer.org support** 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: No file chosen

Checksum: No file chosen

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.

8.5. 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



Protocol	Port	Purpose
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](#).

8.6. 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.

9. Loadbalancing OpenText RightFax – Using Layer 4 DR Mode

9.1. Prepare the OpenText RightFax Servers for Load Balancing

9.1.1. Solve the ARP Problem

If layer 4 DR mode is used, the "ARP problem" must be solved on each load balanced RightFax Server. This enables DR mode to work correctly. The exact steps required depend on the particular operating system in use. The section below detail the steps for Windows 2012 & later. For other operating systems, please refer to [DR Mode Considerations](#) in the Administration Manual.

Windows Server 2012 & Later

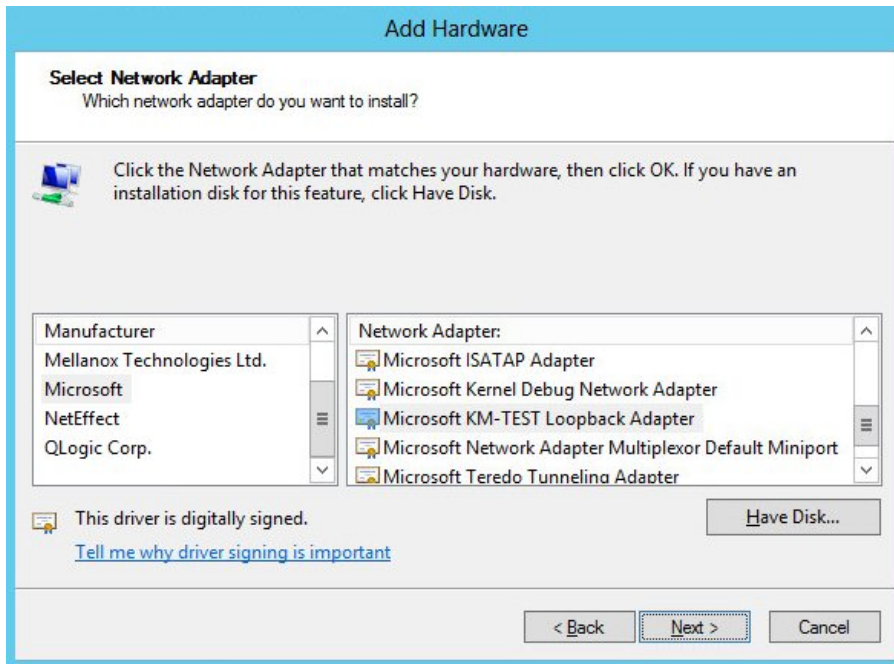
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables the server to receive packets that have their destination set as the VIP address. If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

In addition, the strong/weak host behavior must be configured on each Real Server. The weak host model allows packets with any IP to be sent or received via an interface. The strong host model only allows packets with an IP belonging to the interface to be sent or received.

Important The following 3 steps must be completed on **all** Real Servers associated with the VIP.

Step 1 of 3: Install the Microsoft Loopback Adapter

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
2. Once the Wizard has started, click **Next**.
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**.
4. Select **Network adapters**, click **Next**.



5. Select **Microsoft & Microsoft KM-Test Loopback Adapter**, click **Next**.
6. Click **Next** to start the installation, when complete click **Finish**.

Step 2 of 3: Configure the Loopback Adapter

1. Open Control Panel and click **Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click the new Loopback Adapter and select **Properties**.

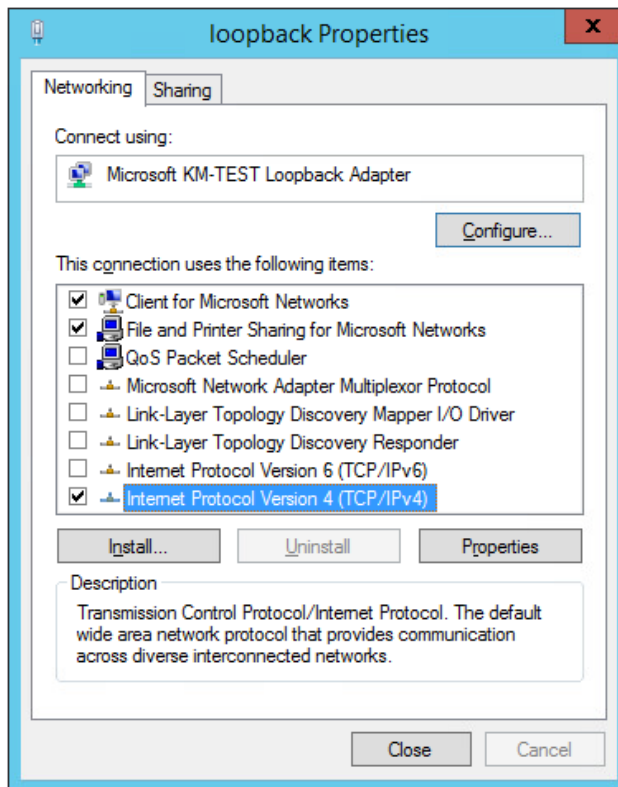
Note You can configure IPv4 or IPv6 addresses or both depending on your requirements.

Important When configuring the loopback adapter properties, make sure that **Client for Microsoft Networks** and **File & Printer Sharing for Microsoft Networks** is also checked as shown below.

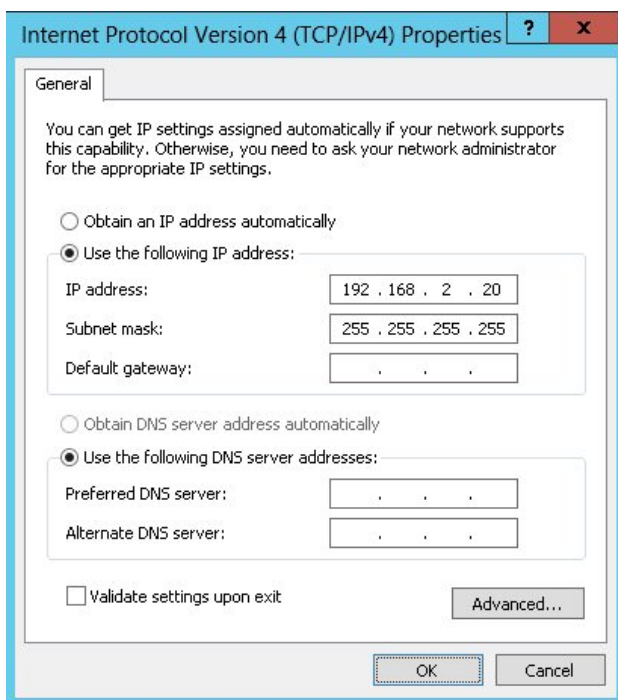
IPv4 Addresses

1. Uncheck all items except **Client for Microsoft Networks**, **File & Printer Sharing for Microsoft Networks** and **Internet Protocol Version 4 (TCP/IPv4)** as shown below:





2. Ensure that **Internet Protocol Version (TCP/IPv4)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service address (VIP) with a subnet mask of **255.255.255.255**, e.g. **192.168.2.20/255.255.255.255** as shown below:



Note

192.168.2.20 is an example, make sure you specify the correct VIP address.



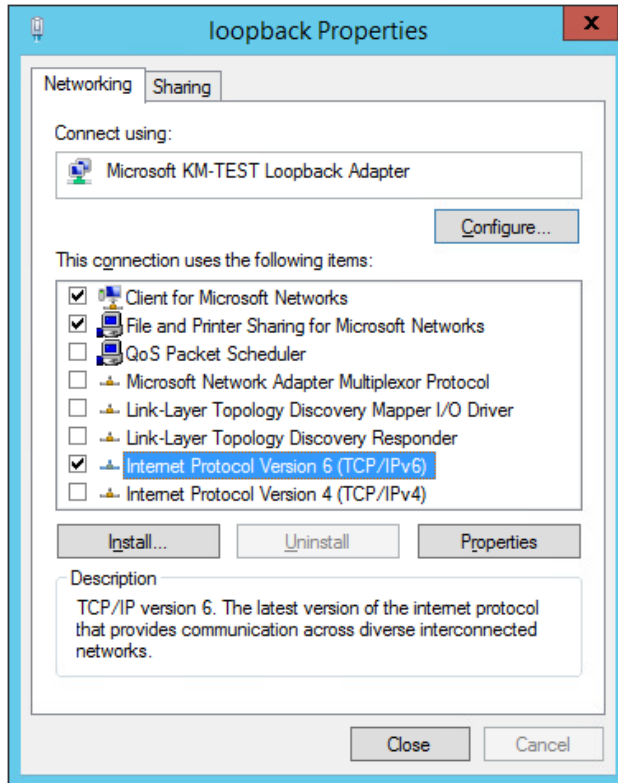
Note

If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

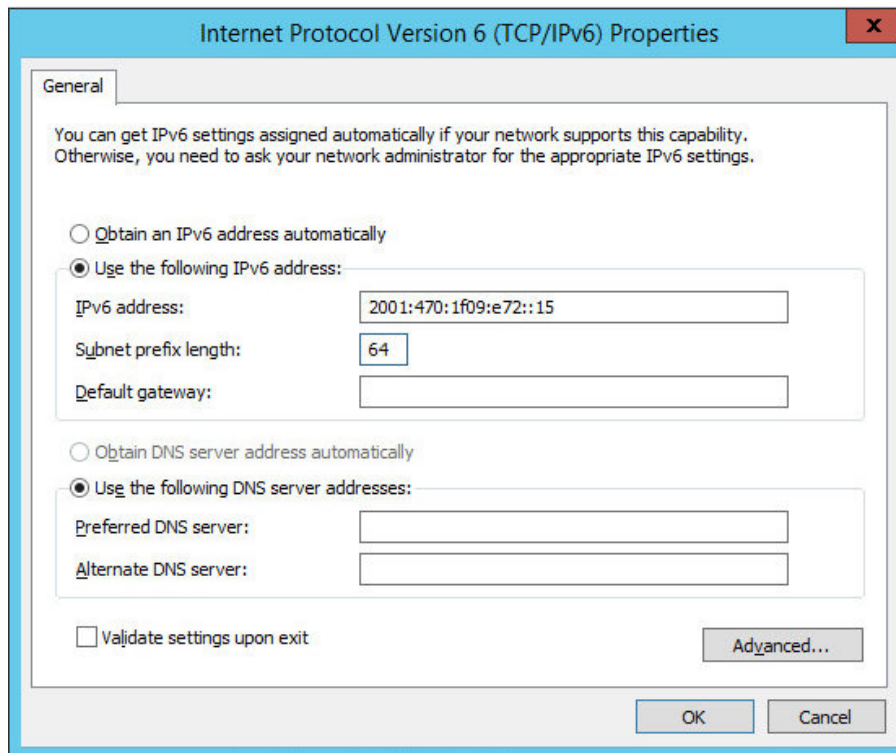
3. Click **OK** then click **Close** to save and apply the new settings.

IPv6 Addresses

1. Uncheck all items except **Client for Microsoft Networks**, **File & Printer Sharing for Microsoft Networks** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:



2. Ensure that **Internet Protocol Version (TCP/IPv6)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) and set the **Subnet Prefix Length** to be the same as your network setting, e.g. **2001:470:1f09:e72::15/64** as shown below:



Note 2001:470:1f09:e72::15/64 is an example, make sure you specify the correct VIP address.

Note If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

3. Click **OK** then click **Close** to save and apply the new settings.

Step 3 of 3: Configure the strong/weak host behavior

The strong/weak host behavior can be configured using either of the following 2 methods:

- Option 1 - Using Network Shell (netsh) commands
- Option 2 - Using PowerShell cmdlets

The commands in this section assume that the LAN Adapter is named "**net**" and the Loopback Adapter is named "**loopback**" as shown in the example below:



Important Either adjust the commands to use the names allocated to your LAN and loopback adapters, or rename the adapters before running the commands. Names are case sensitive so make sure

that the interface names used in the commands match the adapter names exactly.

Option 1 - Using Network Shell (netsh) Commands

To configure the correct strong/weak host behavior run the following commands:

For IPv4 addresses:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmits=0
```

Option 2 - Using PowerShell Cmdlets

For IPv4 addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv4
```

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4
```

For IPv6 Addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv6
```

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6
```

9.1.2. Enable Print and Document Server Load Balancing

When load balancing Microsoft print and document servers, a number of additional configuration steps must be followed to allow them to be load balanced and accessed via a shared name. The exact steps required depend on the particular version of Windows Server being used as detailed below.

Pre-Requisites

1. Each Server must be joined to the same domain as the client PCs.



2. Each Server must have the **Print and Document Service** role installed.
3. All printers must be installed & shared on each Server using exactly the same share names, settings and permissions.

Note

A number of issues have been reported when using Type 4 print drivers, so whenever possible we recommend using Type 3 drivers. Type 4 drivers are usually bundled with the operating system or are downloaded from Windows update, whereas Type 3 drivers are typically downloaded from the printer manufacturer's website.

Enable access via Hostname

To enable the load balanced Print and Document Servers to be accessed via an appropriate hostname, complete the following steps:

Note

The configuration steps below assume the hostname for the VIP is **faxserver-vip** and the domain name is **lbtestdom.com**. Change these to suit your environment.

Windows 2019 & Later

For Windows 2019 & later, local host file entries and a single Registry Key must be added to each Server:

1. Add the following host entries to the local hosts file on each Server:

```
<Real Server IP address> faxserver-vip
<Real Server IP address> faxserver-vip.lbtestdom.com
```

For example, if you have 2 Print and Document Servers - 192.168.100.20 and 192.168.100.21, the following entries must be added:

On the 192.168.100.20 server:

```
192.168.100.20 faxserver-vip
192.168.100.20 faxserver-vip.lbtestdom.com
```

On the 192.168.100.21 server:

```
192.168.100.21 faxserver-vip
192.168.100.21 faxserver-vip.lbtestdom.com
```

2. Add the following Registry Key to each Server:

Note

In the example presented here, **faxserver-vip** is the hostname that will be used to access the load balanced Servers via the virtual service (VIP) created on the load balancer. This can be set to be any appropriate name, although whatever name is used, it must be the **same name** that is used for the DNS entry described in the "Configure DNS Name

Resolution" section below.

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: **OptionalNames**
Type: REG_MULTI_SZ
Data: **faxserver-vip**

Windows 2012 & 2016

For Windows 2012 & 2016, the following Registry Keys must be added to each Server:

Note

In the example presented here, **faxserver-vip** is the hostname that will be used to access the load balanced Servers via the virtual service (VIP) created on the load balancer. This can be set to be any appropriate name, although whatever name is used, it must be the **same name** that is used for the DNS entry described in the "Configure DNS Name Resolution" section below.

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Value: **DisableLoopbackCheck**
Type: REG_DWORD
Data: **1**

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: **DisableStrictNameChecking**
Type: REG_DWORD
Data: **1**

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: **OptionalNames**
Type: REG_MULTI_SZ
Data: **faxserver-vip**

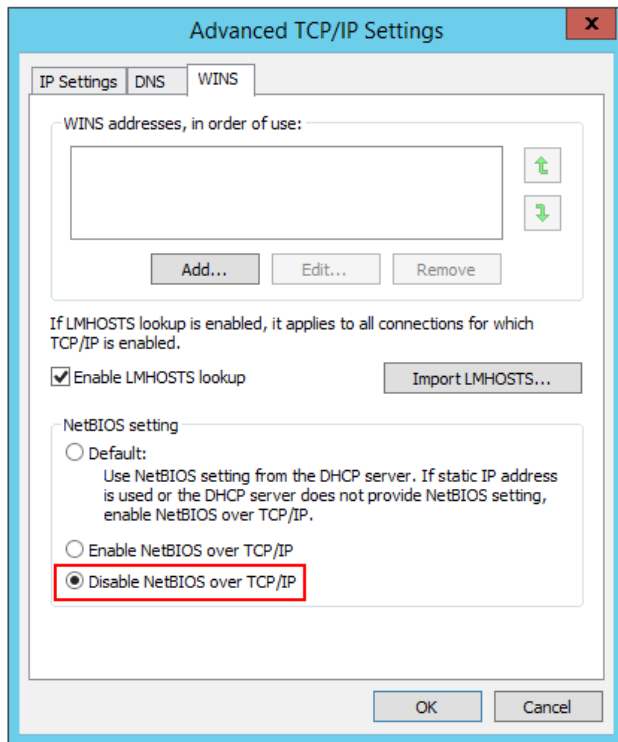
Configure DNS Name Resolution

1. Create a DNS Host (A) record that points to the VIP address. The hostname used must match the value set for the REG_MULTI_SZ **OptionalNames** registry entry, in this example: **faxserver-vip** → **192.168.85.140**.

Disable NetBIOS over TCP/IP

1. On each Server, disable NetBIOS over TCP/IP on **all** interfaces:





Server Reboot

To apply the changes, reboot each Server.

9.2. Configure the Virtual Services

9.2.1. 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**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the virtual service.

Layer 4 - Add a new Virtual Service

Virtual Service		
Label	<input type="text" value="access_http"/>	?
IP Address	<input type="text" value="192.168.85.140"/>	?
Ports	<input type="text" value="80"/>	?
Protocol		
Protocol	<input type="text" value="TCP"/>	?
Forwarding		
Forwarding Method	<input type="text" value="Direct Routing"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

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

Defining the Real Servers (RIPs)

- 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.
- Define the *Label* for the real server as required, e.g. **rightfax_server_1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.190**.
- Click **Update**.
- Repeat these steps to add additional RightFax servers as required.

Layer 4 Add a new Real Server - access_http

Label	<input type="text" value="rightfax_server_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.190"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>






9.2.2. 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**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the virtual service.

Layer 4 - Add a new Virtual Service

Virtual Service		
Label	<input type="text" value="access_https"/>	
IP Address	<input type="text" value="192.168.85.140"/>	
Ports	<input type="text" value="443"/>	
Protocol		
Protocol	<input type="text" value="TCP"/>	
Forwarding		
Forwarding Method	<input type="text" value="Direct Routing"/>	
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

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.

Layer 4 Add a new Real Server - access_https

Label	<input type="text" value="rightfax_server_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.190"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

CancelUpdate

9.2.3. 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**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the virtual service.

Layer 4 - Add a new Virtual Service

Virtual Service		
Label	<input type="text" value="net_filestorage"/>	?
IP Address	<input type="text" value="192.168.85.140"/>	?
Ports	<input type="text" value="445,515"/>	?
Protocol		
Protocol	<input type="text" value="TCP"/>	?
Forwarding		
Forwarding Method	<input type="text" value="Direct Routing"/>	?

CancelUpdate






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.

Layer 4 Add a new Real Server - net_filestorage

Label	<input type="text" value="rightfax_server_1"/>	
Real Server IP Address	<input type="text" value="192.168.85.190"/>	
Weight	<input type="text" value="100"/>	
Minimum Connections	<input type="text" value="0"/>	
Maximum Connections	<input type="text" value="0"/>	

9.2.4. 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.

Layer 4 - Add a new Virtual Service

Virtual Service		
Label	<input type="text" value="access_srv_mod"/>	?
IP Address	<input type="text" value="192.168.85.140"/>	?
Ports	<input type="text" value="20-10522,10062,34001,34988"/>	?
Protocol		
Protocol	<input type="text" value="TCP"/>	?
Forwarding		
Forwarding Method	<input type="text" value="Direct Routing"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

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

Defining the Real Servers (RIPs)

- 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.
- Define the *Label* for the real server as required, e.g. **rightfax_server_1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.190**.
- Click **Update**.
- Repeat these steps to add additional RightFax servers as required.

Layer 4 Add a new Real Server - access_srv_mod

Label	<input type="text" value="rightfax_server_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.190"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>






9.2.5. 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**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the virtual service.

Layer 4 - Add a new Virtual Service

Virtual Service		
Label	<input type="text" value="licensing"/>	
IP Address	<input type="text" value="192.168.85.140"/>	
Ports	<input type="text" value="36363"/>	
Protocol		
Protocol	<input type="text" value="TCP"/>	
Forwarding		
Forwarding Method	<input type="text" value="Direct Routing"/>	
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

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.

Layer 4 Add a new Real Server - licensing

Label	<input type="text" value="rightfax_server_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.190"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

CancelUpdate

10. Loadbalancing OpenText RightFax – Using Layer 7 SNAT Mode

10.1. Prepare the OpenText RightFax Servers for Load Balancing

10.1.1. Enable Print and Document Server Load Balancing

When load balancing Microsoft print and document servers, a number of additional configuration steps must be followed to allow them to be load balanced and accessed via a shared name. The exact steps required depend on the particular version of Windows Server being used as detailed below.

Pre-Requisites

1. Each Server must be joined to the same domain as the client PCs.
2. Each Server must have the **Print and Document Service** role installed.
3. All printers must be installed & shared on each Server using exactly the same share names, settings and permissions.

Note

A number of issues have been reported when using Type 4 print drivers, so whenever possible we recommend using Type 3 drivers. Type 4 drivers are usually bundled with the operating system or are downloaded from Windows update, whereas Type 3 drivers are typically downloaded from the printer manufacturer's website.

Enable access via Hostname

To enable the load balanced Print and Document Servers to be accessed via an appropriate hostname, complete the following steps:

Note

The configuration steps below assume the hostname for the VIP is **faxserver-vip** and the domain name is **lbtestdom.com**. Change these to suit your environment.

Windows 2019 & Later



For Windows 2019 & later, local host file entries and a single Registry Key must be added to each Server:

1. Add the following host entries to the local hosts file on each Server:

```
<Real Server IP address> faxserver-vip
<Real Server IP address> faxserver-vip.lbtestdom.com
```

For example, if you have 2 Print and Document Servers - 192.168.100.20 and 192.168.100.21, the following entries must be added:

On the 192.168.100.20 server:

```
192.168.100.20 faxserver-vip
192.168.100.20 faxserver-vip.lbtestdom.com
```

On the 192.168.100.21 server:

```
192.168.100.21 faxserver-vip
192.168.100.21 faxserver-vip.lbtestdom.com
```

2. Add the following Registry Key to each Server:

Note

In the example presented here, **faxserver-vip** is the hostname that will be used to access the load balanced Servers via the virtual service (VIP) created on the load balancer. This can be set to be any appropriate name, although whatever name is used, it must be the **same name** that is used for the DNS entry described in the "Configure DNS Name Resolution" section below.

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: OptionalNames
Type: REG_MULTI_SZ
Data: faxserver-vip
```

Windows 2012 & 2016

For Windows 2012 & 2016, the following Registry Keys must be added to each Server:

Note

In the example presented here, **faxserver-vip** is the hostname that will be used to access the load balanced Servers via the virtual service (VIP) created on the load balancer. This can be set to be any appropriate name, although whatever name is used, it must be the **same name** that is used for the DNS entry described in the "Configure DNS Name Resolution" section below.

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Value: DisableLoopbackCheck
Type: REG_DWORD
```



Data: 1

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: **DisableStrictNameChecking**
Type: REG_DWORD
Data: 1

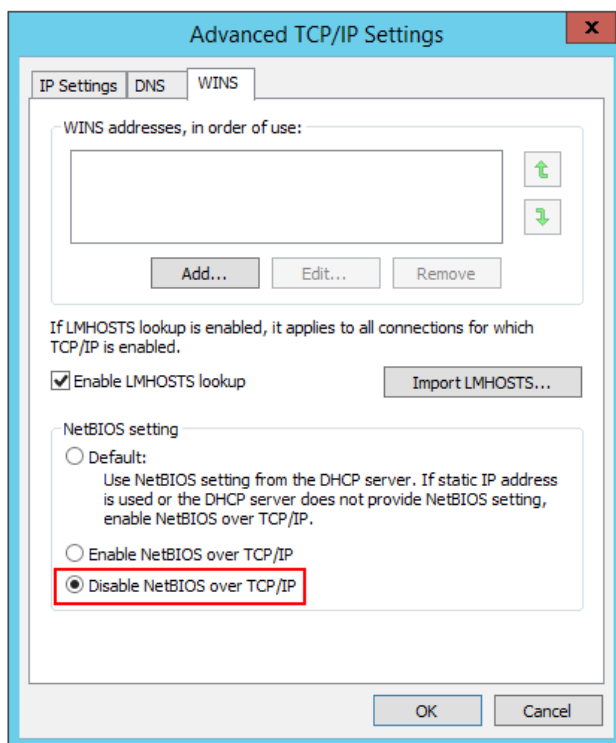
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: **OptionalNames**
Type: REG_MULTI_SZ
Data: **faxserver-vip**

Configure DNS Name Resolution

1. Create a DNS Host (A) record that points to the VIP address. The hostname used must match the value set for the REG_MULTI_SZ **OptionalNames** registry entry, in this example: **faxserver-vip** → **192.168.85.140**.

Disable NetBIOS over TCP/IP

1. On each Server, disable NetBIOS over TCP/IP on **all** interfaces:



Server Reboot

To apply the changes, reboot each Server.

10.2. Configure the Virtual Services

10.2.1. 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. **192.168.85.140**.
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

Virtual Service		[Advanced +]
Label	<input type="text" value="access_http"/>	?
IP Address	<input type="text" value="192.168.85.140"/>	?
Ports	<input type="text" value="80"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

Cancel Update

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_http-1

Label	<input type="text" value="rightfax_server_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.190"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

CancelUpdate

10.2.2. 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. **192.168.85.140**.
4. Set the *Ports* field to **443**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.

Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="access_https"/>	?
IP Address	<input type="text" value="192.168.85.140"/>	?
Ports	<input type="text" value="443"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

CancelUpdate

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

Label	<input type="text" value="rightfax_server_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.190"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

10.2.3. 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. **192.168.85.140**.
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.

Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="net_filestorage"/>	?
IP Address	<input type="text" value="192.168.85.140"/>	?
Ports	<input type="text" value="445,515"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

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 - net_filestorage-1

Label	<input type="text" value="rightfax_server_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.190"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

10.2.4. 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. **192.168.85.140**.
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

Virtual Service		[Advanced +]
Label	<input type="text" value="access_srv_mod"/>	?
IP Address	<input type="text" value="192.168.85.140"/>	?
Ports	<input type="text" value="10520-10522,10062,34001,3"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

Cancel
Update

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_srv_mod-1

Label	<input type="text" value="rightfax_server_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.190"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

CancelUpdate

10.2.5. 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. **192.168.85.140**.
4. Set the *Ports* field to **36363**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.

Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="licensing"/>	?
IP Address	<input type="text" value="192.168.85.140"/>	?
Ports	<input type="text" value="36363"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

CancelUpdate

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 - licensing-1

Label	<input type="text" value="rightfax_server_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.190"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

10.3. 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**.

11. Testing & Verification

Note

For additional guidance on diagnosing and resolving any issues you may have, please also refer to [Diagnostics & Troubleshooting](#).

11.1. 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:

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE	
↑	access_http	192.168.85.140	80	0	TCP	Layer 4	DR	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
↑	rightfax_server_1	192.168.85.190	80	100	0	Drain	Halt	
↑	rightfax_server_2	192.168.85.191	80	100	0	Drain	Halt	
↑	access_https	192.168.85.140	443	0	TCP	Layer 4	DR	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
↑	rightfax_server_1	192.168.85.190	443	100	0	Drain	Halt	
↑	rightfax_server_2	192.168.85.191	443	100	0	Drain	Halt	
↑	net_filestorage	192.168.85.140	445,515	0	TCP	Layer 4	DR	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
↑	rightfax_server_1	192.168.85.190	445,515	100	0	Drain	Halt	
↑	rightfax_server_2	192.168.85.191	445,515	100	0	Drain	Halt	
↑	access_srv_mod	192.168.85.140	10062,340..	0	TCP	Layer 4	DR	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
↑	rightfax_server_1	192.168.85.190	10062,3400..	100	0	Drain	Halt	
↑	rightfax_server_2	192.168.85.191	10062,3400..	100	0	Drain	Halt	
↑	licensing	192.168.85.140	36363	0	TCP	Layer 4	DR	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
↑	rightfax_server_1	192.168.85.190	36363	100	0	Drain	Halt	
↑	rightfax_server_2	192.168.85.191	36363	100	0	Drain	Halt	

12. 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.

13. Further Documentation

For additional information, please refer to the [Administration Manual](#).

14. Appendix

14.1. 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.

14.1.1. 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	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.


14.1.2. 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**.

Create a Clustered Pair

 **LOADBALANCER**

Local IP address

192.168.110.40

IP address of new peer

192.168.110.41


Password for *loadbalancer* user on peer

••••••••••

Add new node

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:


Create a Clustered Pair

 **LOADBALANCER**

Primary

IP: 192.168.110.40

Attempting to pair..

 **LOADBALANCER**

Secondary

IP: 192.168.110.41

Local IP address

192.168.110.40

IP address of new peer

192.168.110.41

Password for *loadbalancer* user on peer


••••••••••


configuring

6. Once complete, the following will be displayed on the Primary appliance:




High Availability Configuration - primary


 **LOADBALANCER**



Primary

IP: 192.168.110.40

 **LOADBALANCER**



Secondary

IP: 192.168.110.41

Break Clustered Pair

- 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](#).

15. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	26 August 2021	Initial version		NH, AH
1.1.0	14 January 2022	<p>Add additional required ports for the "server module access" VIP</p> <p>Add additional required VIP for "licensing"</p> <p>Update diagrams and screenshots to reflect new ports and VIPs</p>	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	<p>Combined software version information into one section</p> <p>Added one level of section numbering</p> <p>Added software update instructions</p> <p>Added table of ports used by the appliance</p> <p>Reworded 'Further Documentation' section</p>	Housekeeping across all documentation	AH
1.1.3	2 February 2023	Updated screenshots	Branding update	AH
1.1.4	7 March 2023	<p>Added the section "Finalizing the Configuration" to ensure HAProxy is explicitly reloaded</p> <p>Removed conclusion section</p>	<p>Provided clarity for reloading HAProxy post-configuration</p> <p>Updates across all documentation</p>	AH
1.2.0	24 March 2023	<p>New document theme</p> <p>Modified diagram colours</p>	Branding update	AH
1.2.1	19 February 2025	Modified guide to use common Microsoft Print and Document Server configuration component	Document standardisation	RJC



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](https://twitter.com/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.

