LOADBALANCER

DEPLOYMENT GUIDE

# Load Balancing Kofax ControlSuite®

Version 2.0.1

# Table of Contents

# 1. About this Guide

This guide details the steps required to configure a load balanced Kofax ControlSuite environment (the guide covers Equitrac, Autostore and Output Manager) utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Kofax ControlSuite configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

# 2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Kofax ControlSuite. 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. Kofax ControlSuite

- All versions

# 4. Kofax ControlSuite

Kofax ControlSuite is an integrated print and output management, capture and mobile document workflow solution. ControlSuite combines individual components that work together in various configurations to create multiple document processing workflows. ControlSuite consists of the following main components:

- **Equitrac Print Management** - Equitrac is a print management and cost recovery solution which measures, monitors, and manages document output on the network.
- **AutoStore Document and Image Capture** - AutoStore captures, processes, and routes paper and electronic documents in a business environment.
- **Output Manager** - Output Manager gives organizations control of what, when, and how they produce and deliver information.

- **Business Connect** - Business Connect extends business processes to a mobile device, by adding the Business Connect Server and the Business Connect Client to the core ControlSuite applications.

# 5. Load Balancing Kofax ControlSuite

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

Kofax ControlSuite components & services can be installed on multiple servers and load balanced to provide load sharing and HA. The following sections describe the Virtual Services (VIPs) that are required for Equitrac, AutoStore and Output Manager.

For additional details, refer to ControlSuite component high availability support and ControlSuite communication ports.

> **Note** The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to Configuring HA - Adding a Secondary Appliance for more details on configuring a clustered pair.

## 5.1. Load Balancing Equitrac

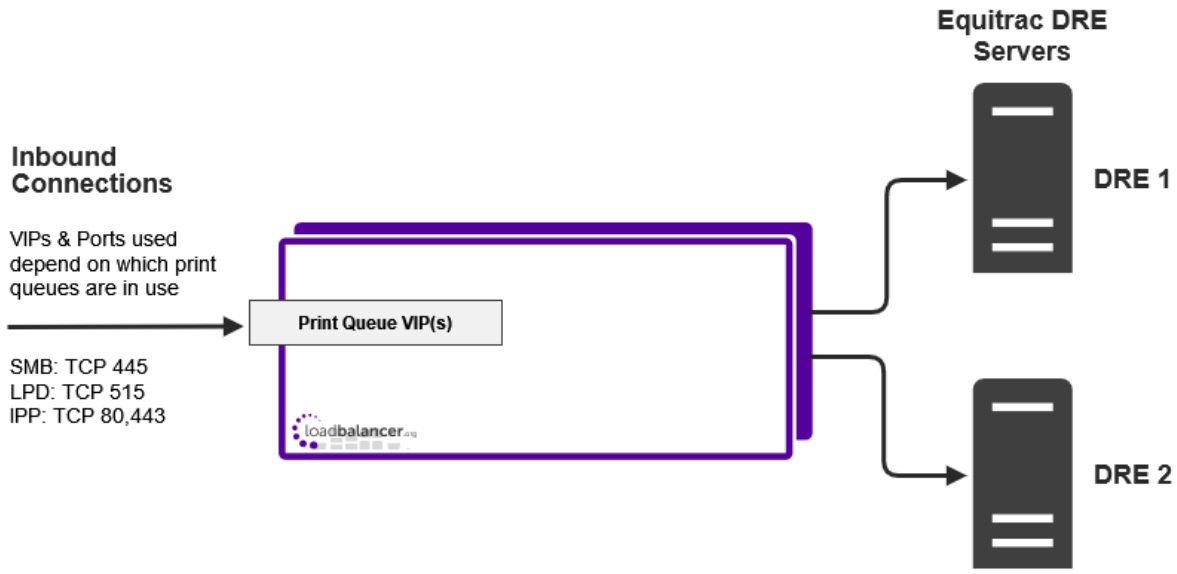
For Equitrac, load balancing is configured for print submission and print release.

### 5.1.1. Print Submission (DRE - Document Routing Engine)

Print submission load balancing & HA provides server level protection and load sharing for the print server and print spooler. The load balancer is located between client workstations and multiple DREs.

> **Note** For more information, please refer to Equitrac Print Submission High Availability for DRE.

**Deployment Concept**



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

### Virtual Service (VIP) Requirements

A VIP must be configured for each type of print queue that's in use.

#### SMB Print Queues

| VIP Name | Mode(s) Supported | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| EQ-DRE-SMBqueues | L4 DR, L4 NAT or L7 SNAT | 445 | Source IP | Connect to Port |

#### LPD Print Queues

| VIP Name | Mode(s) Supported | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| EQ-DRE-LPDqueues | L4 DR, L4 NAT or L7 SNAT | 515 | Source IP | Connect to Port |

#### IPP Print Queues

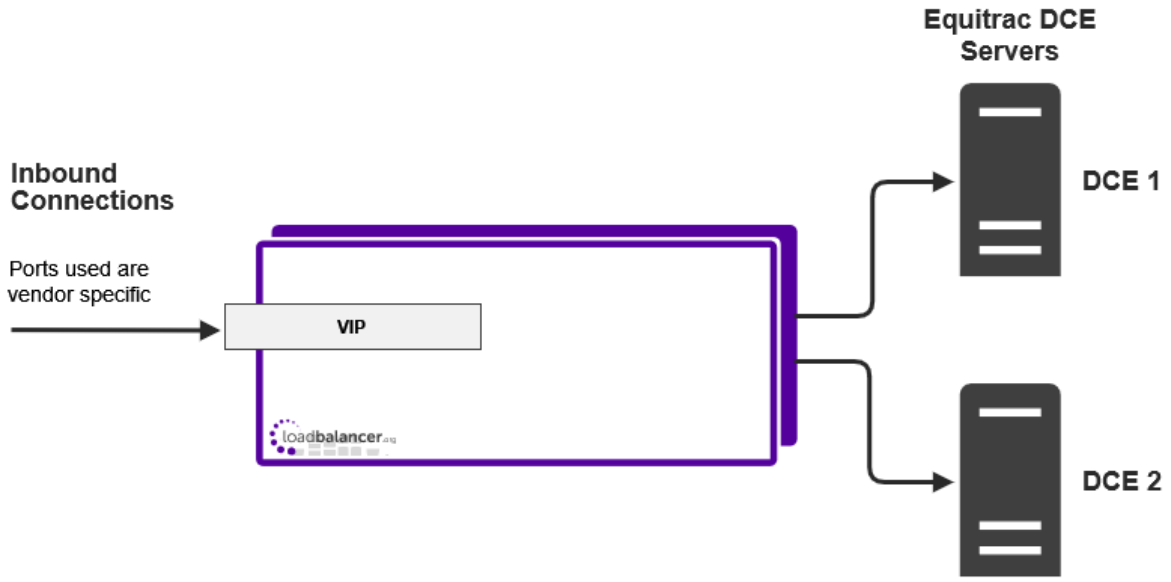
| VIP Name | Mode(s) Supported | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| EQ-DRE-IPPqueues | L4 DR, L4 NAT or L7 SNAT | 80,443 | Source IP | Connect to Port |

## 5.1.2. Print Release (DCE - Device Control Engine)

Print release load balancing & HA provides server level protection and load sharing for the print release workflow. The load balancer is located between the MFP and multiple DCEs.

> **Note** For more information, please refer to Equitrac Print Release High Availability.

### Deployment Concept




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

### 5.1.3. Virtual Service (VIP) Requirements

A single VIP is required, the port(s) to load balance depend on the particular MFP in use.

#### Lexmark / Ricoh

| VIP Name | Mode(s) Supported | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| EQ-DCE-LexRicoh | L4 DR or L4 NAT | 2939 | None | HTTP (GET) |

#### HP OXPd

| VIP Name | Mode(s) Supported | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| EQ-DCE-HP | L4 DR or L4 NAT | 2939,7627 | None | HTTP (GET) |

#### All Ports VIP

Alternatively, an "all ports" VIP can be used if preferred to support all MFPs. This is also useful if your vendor is not listed and you don't know which port(s) to specify.

| VIP Name | Mode | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| EQ-DCE-AllPorts | L4 DR or L4 NAT | * | None | Connect to Port |

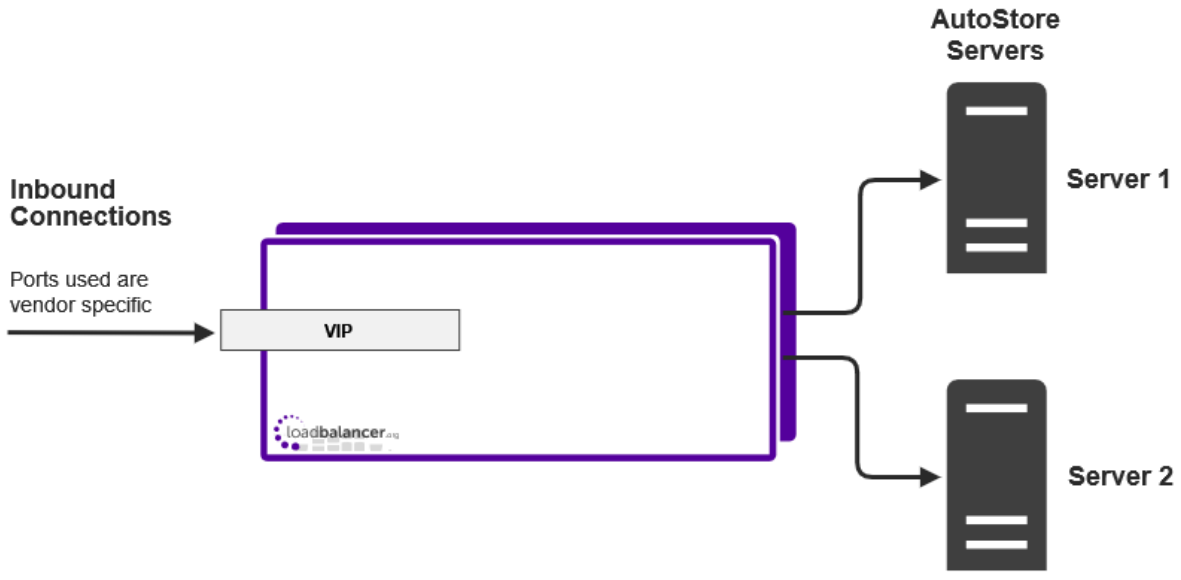
## 5.2. Load Balancing Kofax AutoStore

Multiple Autostore servers can be added to provide HA and load balancing. The load balancer receives requests from the client devices and distributes the requests to the servers.

Each AutoStore server must be configured as a standalone server, making sure the exact same configuration steps are followed on all servers and that they have access to the same configuration and script files.

> **Note** For more information, please refer to Autostore High Availability.

### 5.2.1. Deployment Concept



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

### 5.2.2. Virtual Service (VIP) Requirements

A single VIP is required, the port(s) to load balance depend on the particular MFP in use.

#### Lexmark MFP / HP OXPd / Ricoh Desktop SF

| VIP Name | Mode | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| AS-LexHpRicohDSF | L4 DR or L4 NAT | 3233,3234 | Source IP | Connect to Port |

#### Ricoh ESA

| VIP Name | Mode | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| AS-RicohESA | L4 DR or L4 NAT | 8084,9000 | Source IP | Connect to Port |

#### Ricoh SOP

| VIP Name | Mode | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| AS-RicohSOP | L4 DR or L4 NAT | 3350 | Source IP | Connect to Port |

#### Konica Minolta iOption

| VIP Name | Mode | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| AS-KonicaMinolta | L4 DR or L4 NAT | 3348,3281,13352,13353,13391 | Source IP | Connect to Port |

> **Note** For other MFPs, please refer to AutoStore Communication Ports.

#### All Ports VIP

Alternatively, an "all ports" VIP can be used if preferred to support all MFPs. This is also useful if your vendor is not listed and you don't know which port(s) to specify.

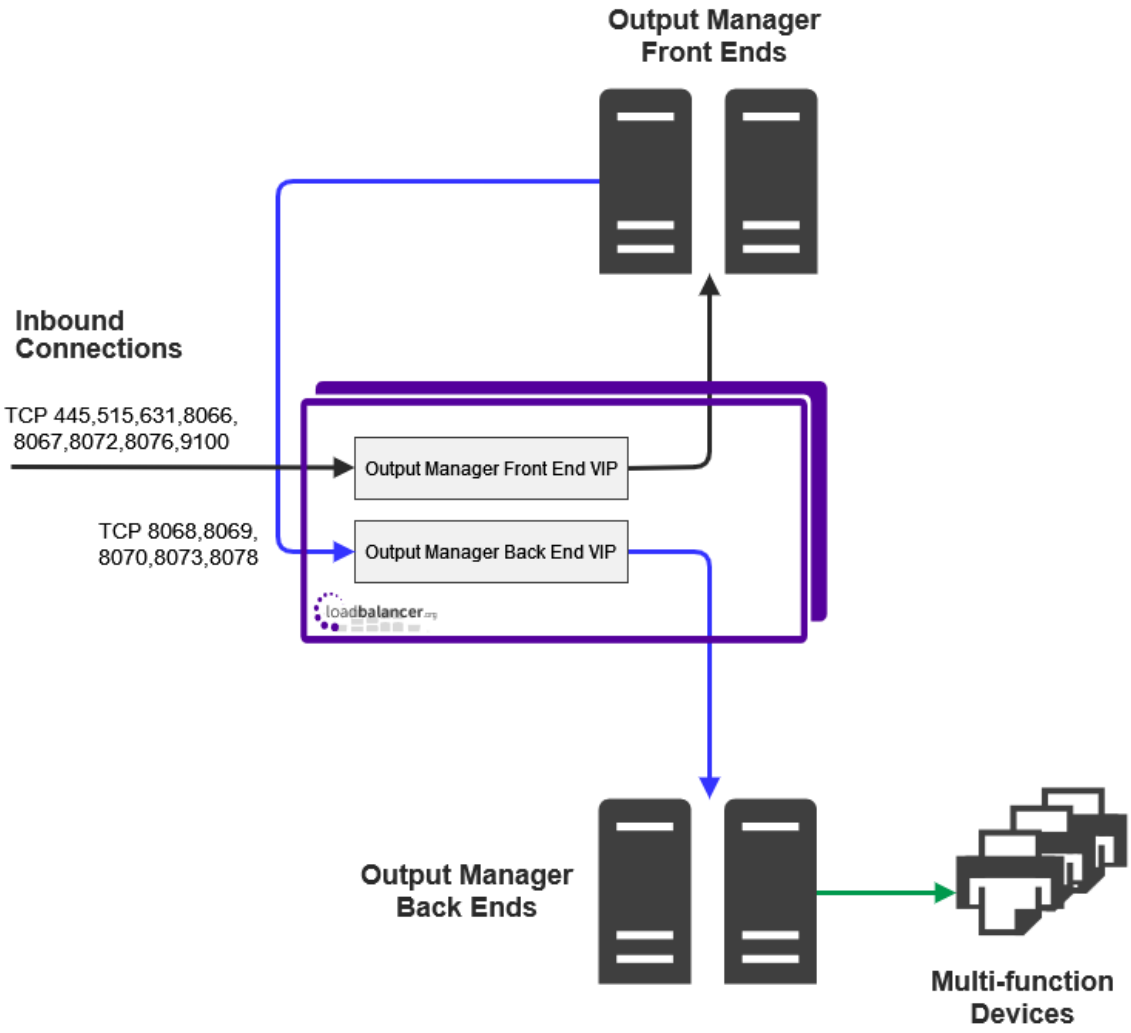
| VIP Name | Mode | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| AS-AllPorts | L4 DR or L4 NAT | * | Source IP | Connect to Port |

## 5.3. Load Balancing Kofax Output Manager

Multiple Output Manager Front-end and Back-end servers can be added to provide HA and load sharing. All front-end servers and all back-end server must be configured in the same way. The load balancer is located between clients and the Front-end servers and between the Front-end servers and the Back-end servers.

> **Note** For more information, please refer to Output Manager in a High Availability Environment.

### 5.3.1. Deployment Concept




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

### 5.3.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for Output Manager, 2 VIPs are required - one for the front-end the other for the back-end.

| VIP Name | Mode | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|
| OM-FrontEnd | L4 DR, L4 NAT or L7 SNAT | 445,515,631,8066, 8067,8072,8076,9100 | None | Connect to Port |
| OM-BackEnd | L4 DR, L4 NAT or L7 SNAT | 8068,8069,8070,8073,8078 | None | Connect to Port |

# 6. 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 Kofax ControlSuite, layer 4 DR mode is recommended and is used for the configurations presented in this guide. If Layer 4 DR mode cannot be used due to Real Server or network topology reasons, then layer 4 NAT mode

is recommended. If this is not appropriate due to network topology reasons (the default gateway of all load balanced servers must be the load balancer), then layer 7 SNAT mode can be used.

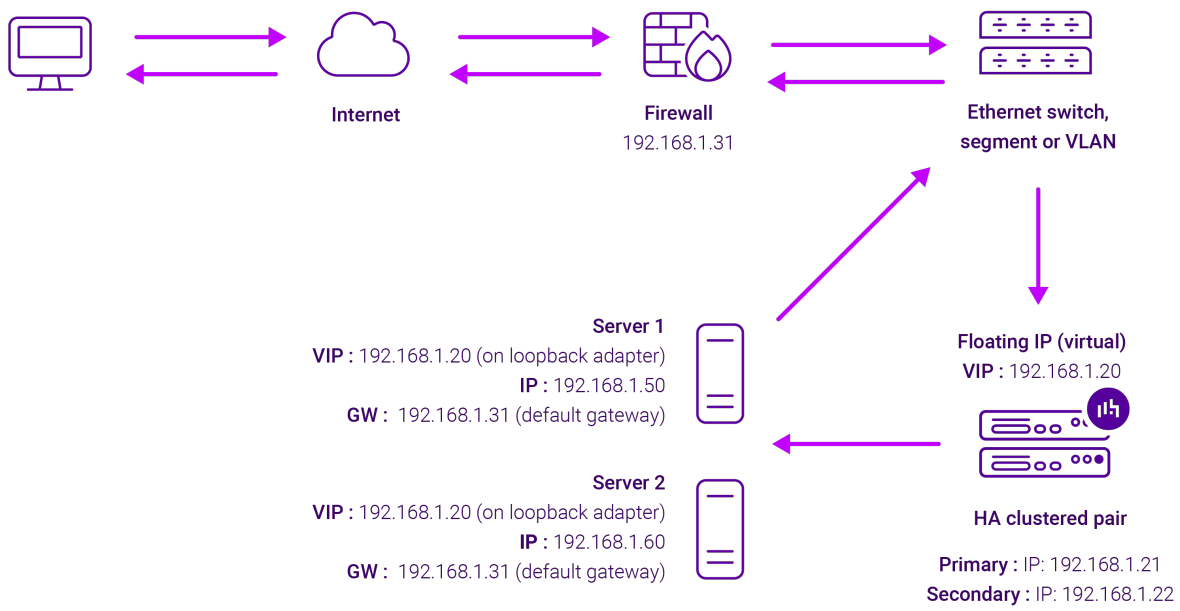
> **Note** Layer 7 SNAT mode cannot be used for Equitrac DCE print release or for AutoStore. In both cases the load balanced servers must see the source IP of the requestor and not the load balancer as would be the case with SNAT mode.

Layer 4 DR mode, Layer 4 NAT mode and layer 7 SNAT mode are described below.

## 6.1. 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***.



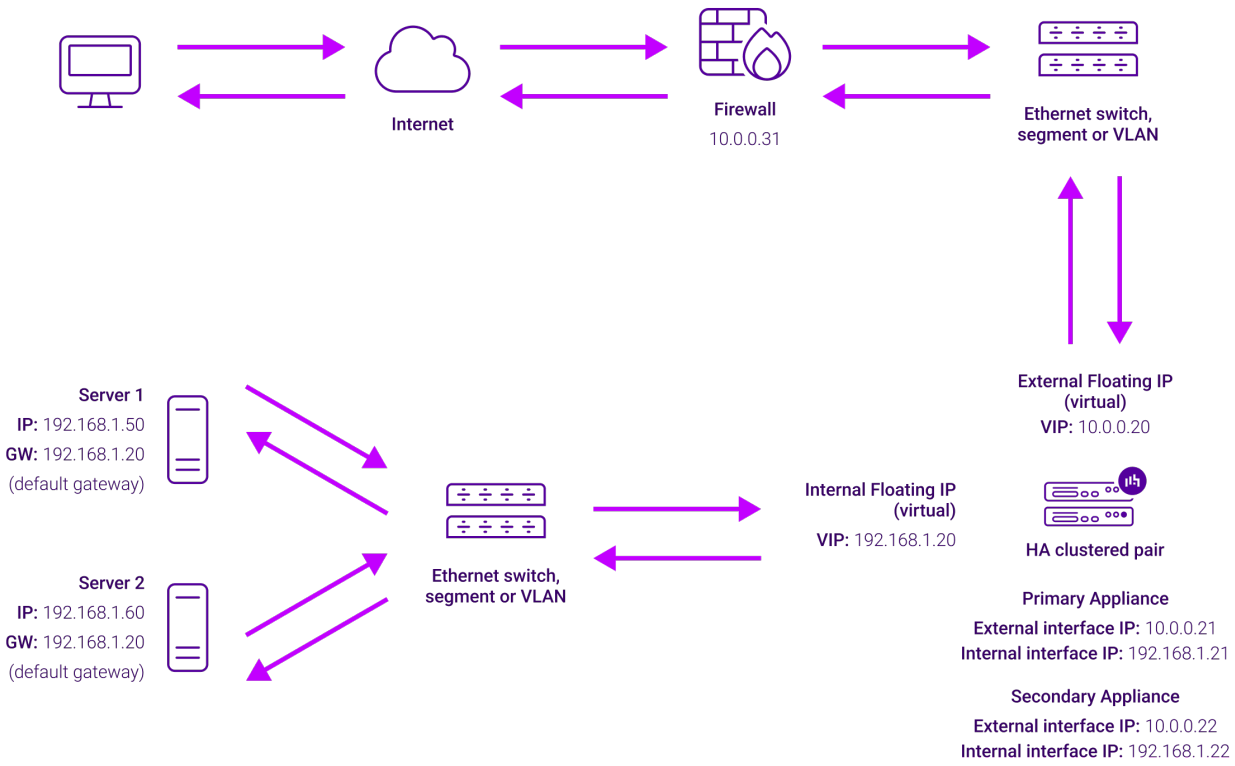

- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that each Real Server (and the 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.

## 6.2. Layer 4 NAT Mode

Layer 4 NAT mode is a high performance solution, although not as fast as layer 4 DR mode. This is because real server responses must flow back to the client via the load balancer rather than directly as with DR mode. The image below shows an example network diagram for this mode.




- The load balancer translates all requests from the Virtual Service to the Real Servers.
- NAT mode can be deployed in the following ways:
  - **Two-arm (using 2 Interfaces)** (as shown above) - Here, 2 subnets are used. The VIP is located in one subnet and the load balanced Real Servers are located in the other. The load balancer requires 2 interfaces, one in each subnet.

> **Note** This can be achieved by using two network adapters, or by creating VLANs on a single adapter.

    - Normally **eth0** is used for the internal network and **eth1** is used for the external network, although this is not mandatory since any interface can be used for any purpose.
    - If the Real Servers require Internet access, *Auto-NAT* should be enabled using the WebUI menu

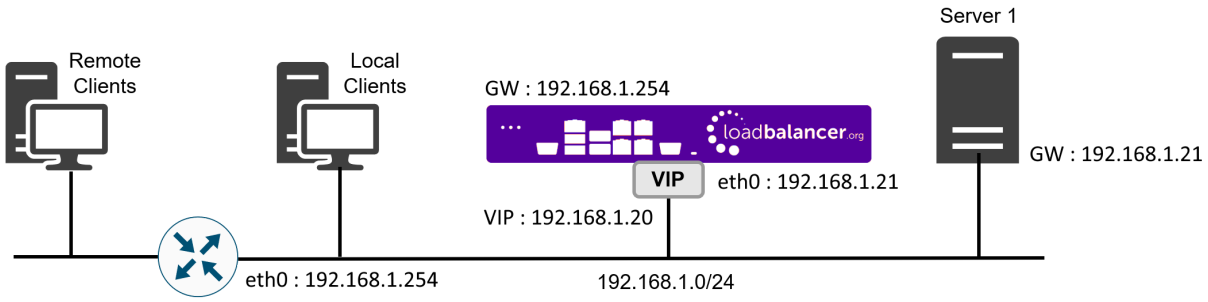
option: *Cluster Configuration > Layer 4 - Advanced Configuration*, the external interface should be selected.

- The default gateway on the Real Servers must be set to be an IP address on the load balancer.

> **Note** For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

- Clients can be located in the same subnet as the VIP or any remote subnet provided they can route to the VIP.

- **One-arm (using 1 Interface)** - Here, the VIP is brought up in the same subnet as the Real Servers.




- To support remote clients, the default gateway on the Real Servers must be an IP address on the load balancer and routing on the load balancer must be configured so that return traffic is routed back via the router.

> **Note** For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

- To support local clients, return traffic would normally be sent directly to the client bypassing the load balancer which would break NAT mode. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer. For more information please refer to One-Arm (Single Subnet) NAT Mode.

- If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this.
- Port translation is possible with Layer 4 NAT mode, e.g. VIP:80 → RIP:8080 is supported.
- NAT mode is transparent, i.e. the Real Server will see the source IP address of the client.

### NAT Mode Packet re-Writing

In NAT mode, the inbound destination IP address is changed by the load balancer from the Virtual Service IP address (VIP) to the Real Server. For outbound replies the load balancer changes the source IP address of the Real Server to be the Virtual Services IP address.

**The following table shows an example NAT mode setup:**

| Protocol | VIP | Port | RIP | Port |
|---|---|---|---|---|
| TCP | 10.0.0.20 | 80 | 192.168.1.50 | 80 |

In this simple example all traffic destined for IP address 10.0.0.20 on port 80 is load-balanced to the real IP address 192.168.1.50 on port 80.

**Packet rewriting works as follows:**

1) The incoming packet for the web server has source and destination addresses as:

| | | | |
|---|---|---|---|
| **Source** | x.x.x.x:34567 | **Destination** | 10.0.0.20:80 |

2) The packet is rewritten and forwarded to the backend server as:

| | | | |
|---|---|---|---|
| **Source** | x.x.x.x:34567 | **Destination** | 192.168.1.50:80 |

3) Replies return to the load balancer as:

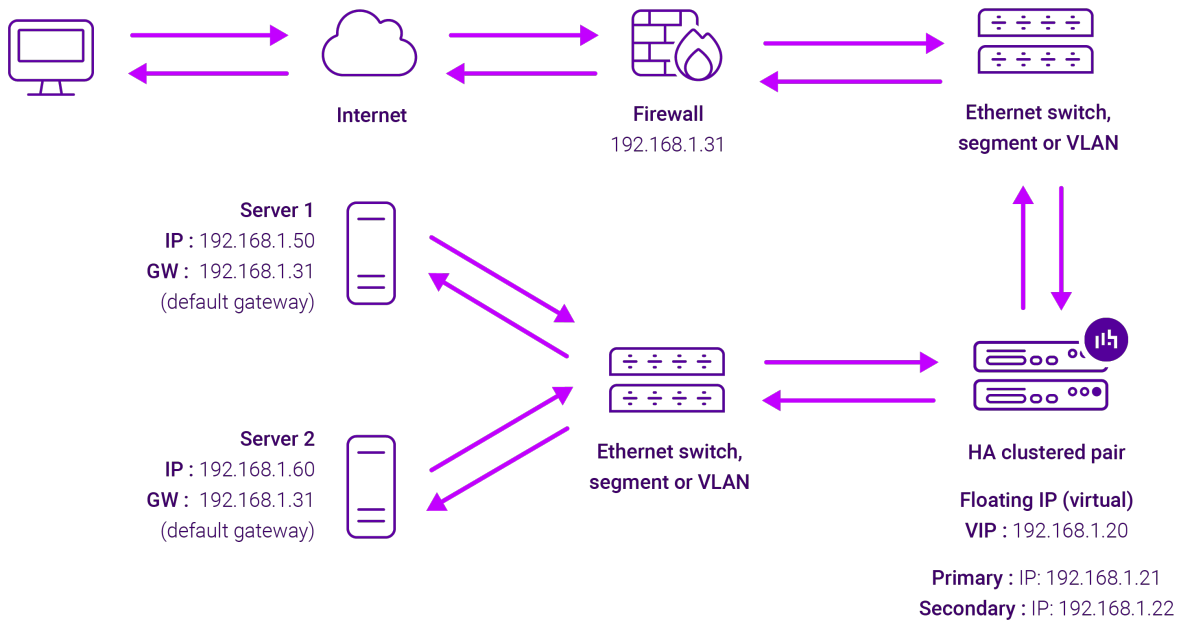
| | | | |
|---|---|---|---|
| **Source** | 192.168.1.50:80 | **Destination** | x.x.x.x:34567 |

4) The packet is written back to the VIP address and returned to the client as:

| | | | |
|---|---|---|---|
| **Source** | 10.0.0.20:80 | **Destination** | x.x.x.x:34567 |

## 6.3. 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. Loadbalancer.org Appliance – the Basics

## 7.1. Virtual Appliance

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.

> **Note** The same download is used for the licensed product, the only difference is that a license key file

(supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

> **Note** Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

> **Note** The VA has 4 network adapters. For VMware only the first adapter (**eth0**) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

## 7.2. Initial Network Configuration

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

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

## 7.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

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

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

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

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

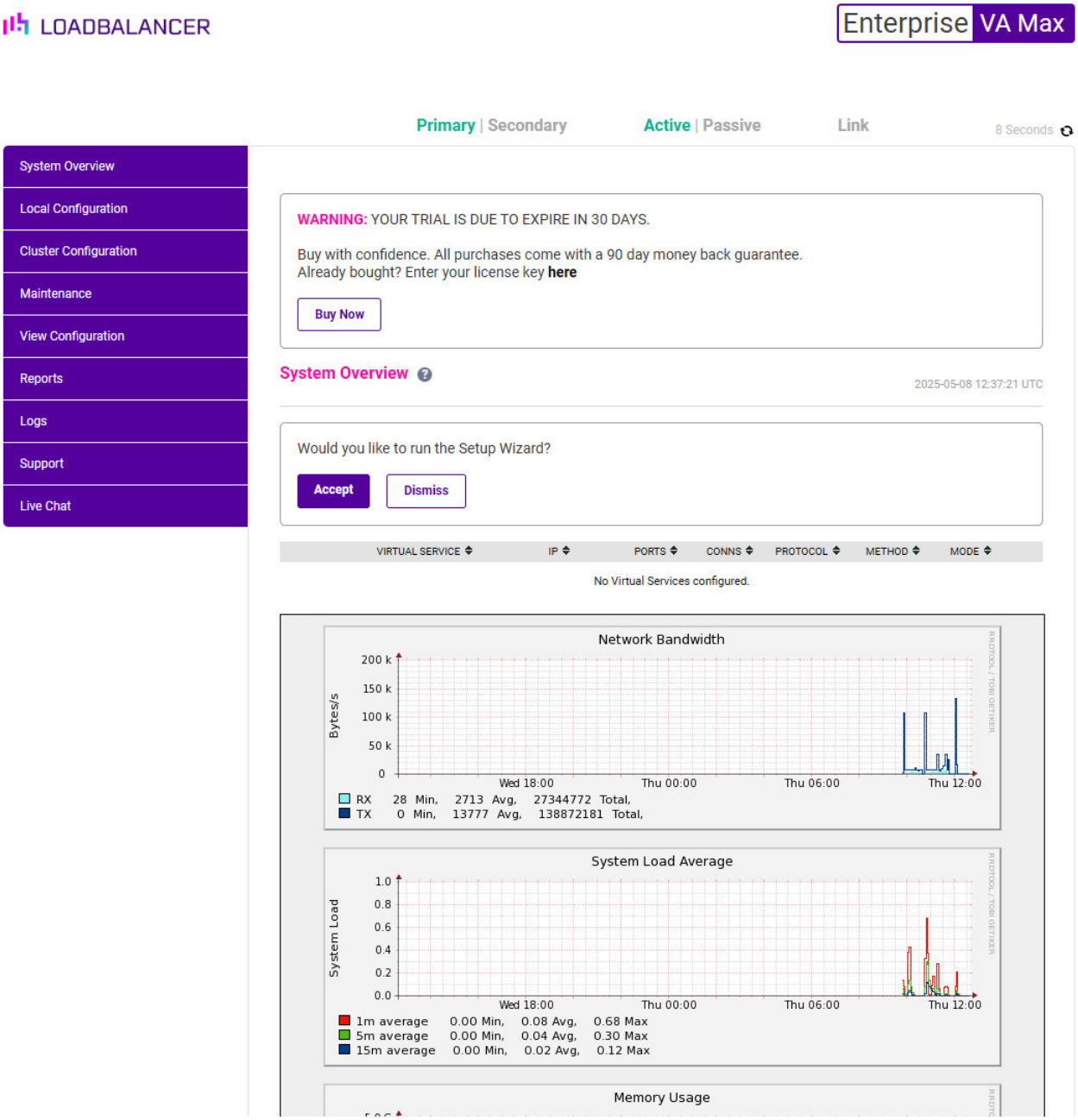
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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

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

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

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




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.

## 7.3.1. Main Menu Options

**System Overview** - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
**Local Configuration** - Configure local host settings such as IP address, DNS, system time etc.
**Cluster Configuration** - Configure load balanced services such as VIPs & RIPs
**Maintenance** - Perform maintenance tasks such as service restarts and creating backups
**View Configuration** - Display the saved appliance configuration settings
**Reports** - View various appliance reports & graphs

**Logs** - View various appliance logs
**Support** - Create a support download, contact the support team & access useful links
**Live Chat** - Start a live chat session with one of our Support Engineers

## 7.4. Appliance Software Update

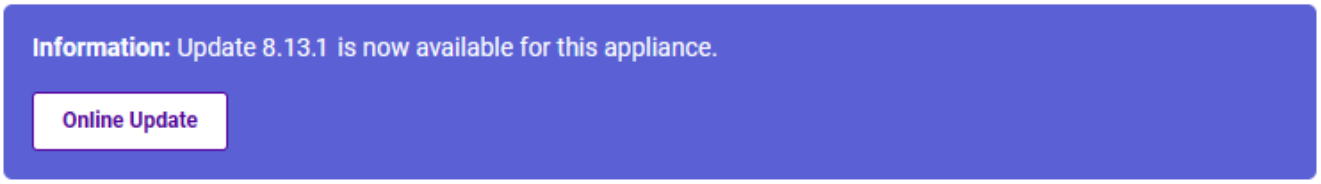
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

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

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

### 7.4.1. Online Update

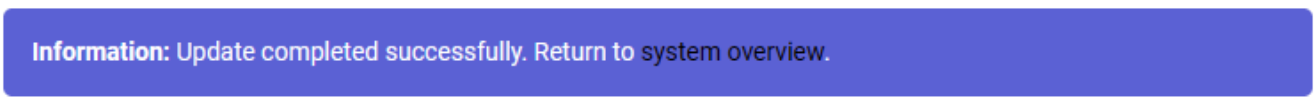
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:




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

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

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




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

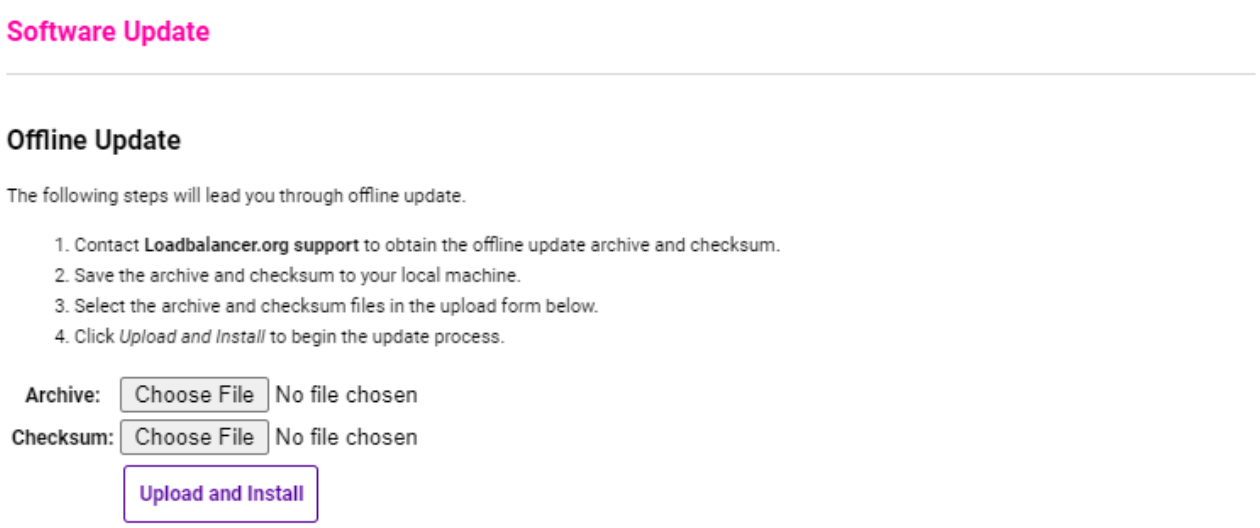
### 7.4.2. Offline Update

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

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

To perform an offline update:

1. Using the WebUI, navigate to: *Maintenance > Software Update*.
2. Select **Offline Update**.
3. The following screen will be displayed:




4. Select the *Archive* and *Checksum* files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

## 7.5. Ports Used by the Appliance

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

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

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

## 7.6. HA Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in the section Configuring HA - Adding a Secondary Appliance of the appendix.

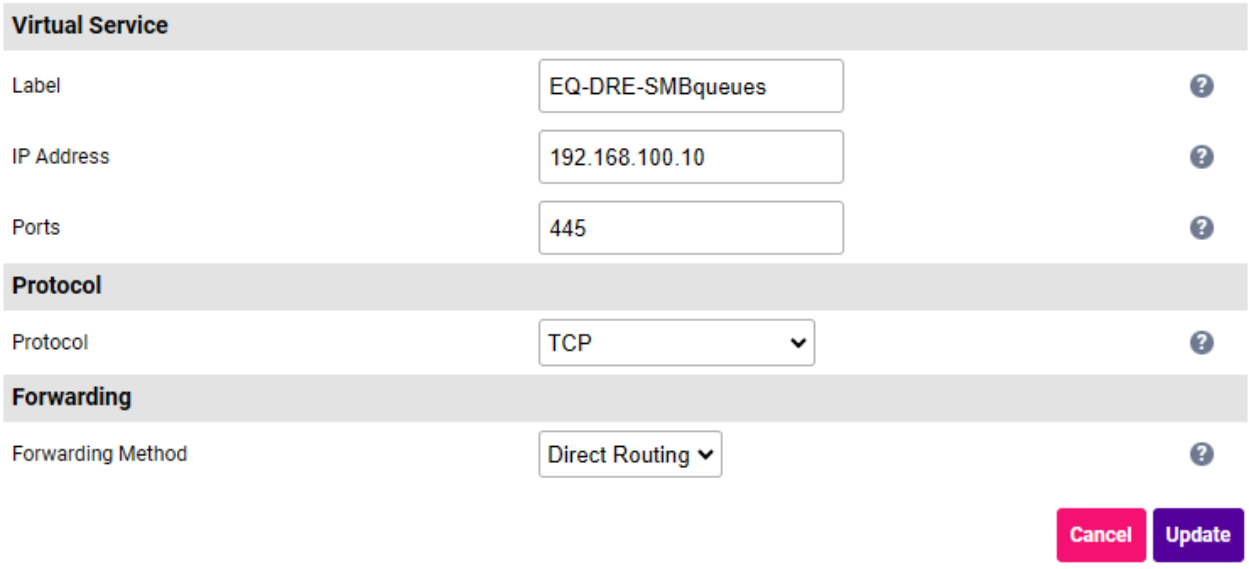
# 8. Configuring Load Balancing for Kofax Equitrac

## 8.1. Appliance Configuration

### 8.1.1. Print Submission

#### Configure the Virtual Service (VIP)

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

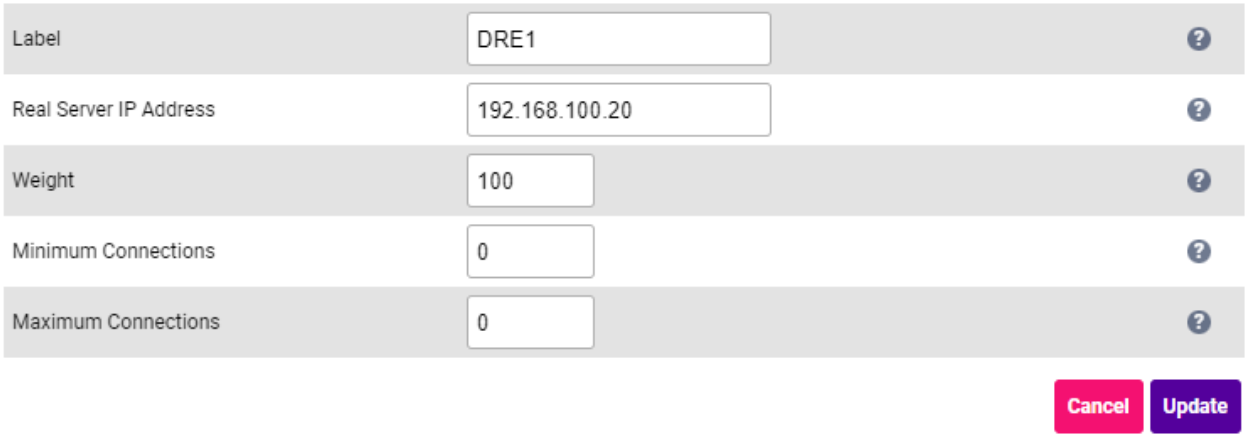



   - Specify an appropriate *Label* for the Virtual Service, e.g. **EQ-DRE-SMBqueues**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.100.10**.
   - Set the *Ports* field to **445**.
   - Ensure that the *Protocol* is set to **TCP**.
   - Ensure that the *Forwarding Method* is set to **Direct Routing**.
3. Click **Update**.
4. Now click **Modify** next to the newly created VIP.

5. Scroll to the *Health Checks* section.
    - Set the *Check Port* to **2938**.
6. Click **Update**.

### Define the Associated Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.



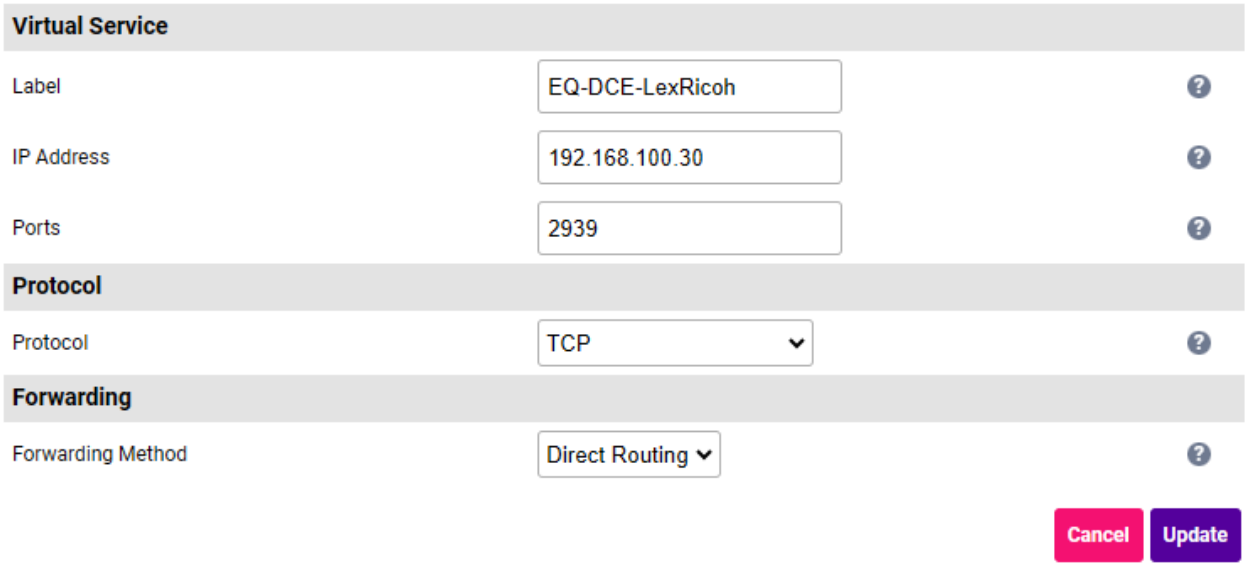

    - Specify an appropriate *Label* for the Real Server, e.g. **DRE1**.
    - Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.100.20**.
2. Click **Update**.
3. Repeat these steps to add additional DRE servers.

> **Note** To configure VIPs for IPP or LPD print queues, repeat the above steps using the same IP address and specify either ports **443** & **80** (for IPP) or **515** (for LPD) rather than **445**.

## 8.1.2. Print Release

### Configure the Virtual Service (VIP)

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

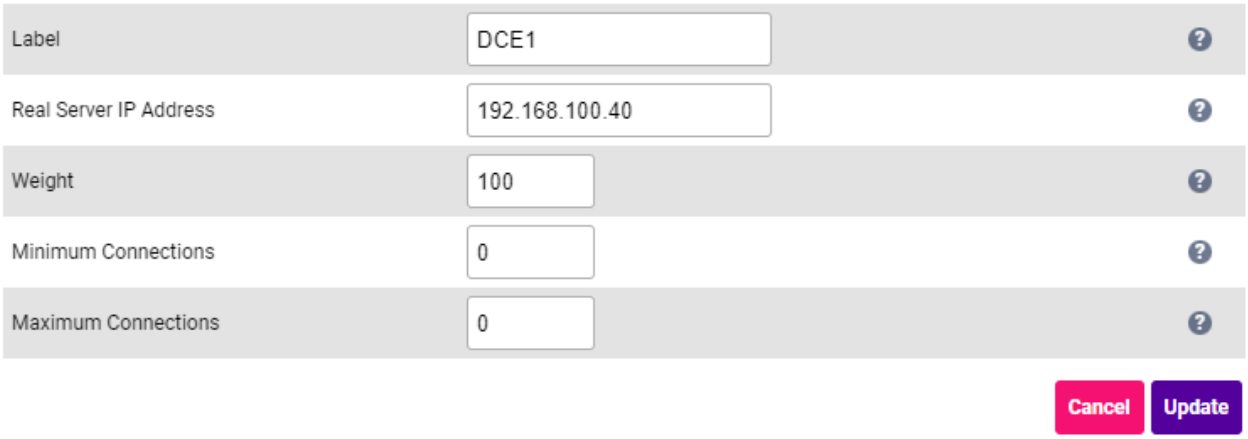



- Specify an appropriate *Label* for the Virtual Service, e.g. **EQ-DCE-LexRicoh**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.100.30**.
- Set the *Ports* field according to your MFP vendor:
  - For Lexmark and Ricoh, specify port **2939**
  - For HP OXPd, specify ports **2939** and **7627**
  - If you're not sure of which ports are used by your MFP, an "all ports" VIP can be used as mentioned in Load Balancing Equitrac. For this specify ***** (i.e. an asterisk).
- Ensure that the *Protocol* is set to **TCP**.
- Ensure that the *Forwarding Method* is set to **Direct Routing**.

3. Click **Update**.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Persistence* section.
   - Clear the *Enable* checkbox to disable persistence.
6. Scroll to the *Health Checks* section.
   - Set the *Check Port* to **2939**.
7. Click **Update**.

## Define the Associated Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.




- Specify an appropriate *Label* for the Real Server, e.g. **DCE1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.100.40**.

2. Click **Update**.
3. Repeat these steps to add additional DCE servers.

## 8.2. Kofax Equitrac Configuration

### 8.2.1. Device Registration Service Configuration

Use Device Registration Service (DRS) to ensure that all required MFP clients are defined/installed.

### 8.2.2. DRE Configuration

#### Configure each DRE to only return the Production IP Address

When using layer 4 DR mode, a system environment variable must be added to each DRE server so that it only sends its production IP Address (and not the IP address on the loopback adapter) as part of the service registration message. To do this, follow the steps below:

1. Go to **Control Panel > All Control Panel Items > System** on the DRE server, and select **Advanced system settings**.
2. On the System properties window, click **Environmental Variables**.
3. On the Environment Variables window, click **New** from the System variables section.
4. Create the Variable name **EQ_IPADDRESSES** with a Variable value of the production IP Address of your Equitrac DRE server, and press **OK** and then **OK** again.
5. Repeat these steps above for each DRE server in your deployment.

> **Note** For more information, please refer to Add the IP address variable.

#### Solve the ARP Problem

When using layer 4 DR mode, the "ARP Problem" must be solved on each DRE Server to enable DR mode to work correctly. The exact steps required depend on the particular operating system in use. To solve the ARP problem for Windows 2012 and later, please refer to Solving the ARP Problem in the appendix.

## 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 **PrintLB** 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> PrintLB
<Real Server IP address> PrintLB.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 PrintLB
192.168.100.20 PrintLB.lbtestdom.com
```

**On the 192.168.100.21 server:**

```
192.168.100.21 PrintLB
192.168.100.21 PrintLB.lbtestdom.com
```

2. Add the following Registry Key to each Server:

> **Note**
>
> In the example presented here, **PrintLB** 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: PrintLB
```

### Windows 2012 & 2016

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

> **Note**
>
> In the example presented here, **PrintLB** 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
```

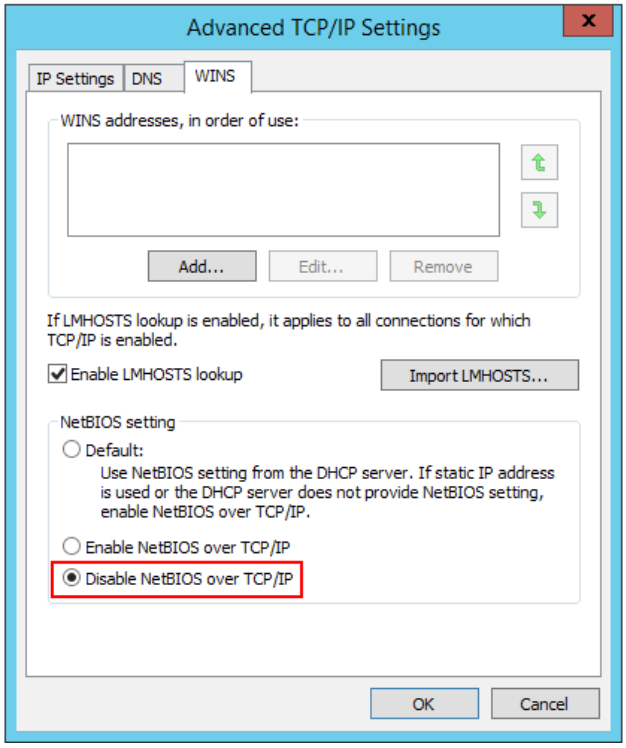
```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: OptionalNames
Type: REG_MULTI_SZ
Data: PrintLB
```

#### 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: **PrintLB → 192.168.100.10**.

#### 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.

> **Note** The DNS Host (A) record created above (PrintLB) is the hostname that end users connect to from their workstations to map to the Follow-You Queue (e.g. \\PrintLB\FollowYouPrinting).

## 8.2.3. DCE Configuration

### Configure for High Availability

When multiple DCEs are installed, they must be configured for HA as detailed below:

1. Install ControlSuite with DCE and run the ConfigAssistant.
2. On the **Services** page click the "..." button beside **Device Control Engine**, and select **Virtual Site Name** from the list.
3. Enter the **virtual site name** that matches the VIP of the NLB, and click **OK**.
4. On the **Services** page click the "..." button beside **Device Control Engine**, and select **Start** from the list.
5. Continue configuring ControlSuite.

> **Note** For more information, please refer to Install DCE in an high availability setup.

### Solve the ARP Problem

When using layer 4 DR mode, the "ARP Problem" must be solved on each DCE and DRE Server to enable DR mode to work correctly. The exact steps required depend on the particular operating system in use. To solve the ARP problem for Windows 2012 and later, please refer to Solving the ARP Problem in the appendix.

> **Note** If DCE and DRE are installed on the same server, simply add a second IP address to the loopback adapter that corresponds to the print release VIP.

## 8.3. Load Balanced Print Queue Testing & Verification

You should now be able to access your printers using either the Virtual Service IP address or the share name. In the example presented in this guide, either:

```
\\192.168.100.10
```

or

```
\\PrintLB
```

or

```
\\PrintLB.lbtestdom.com
```

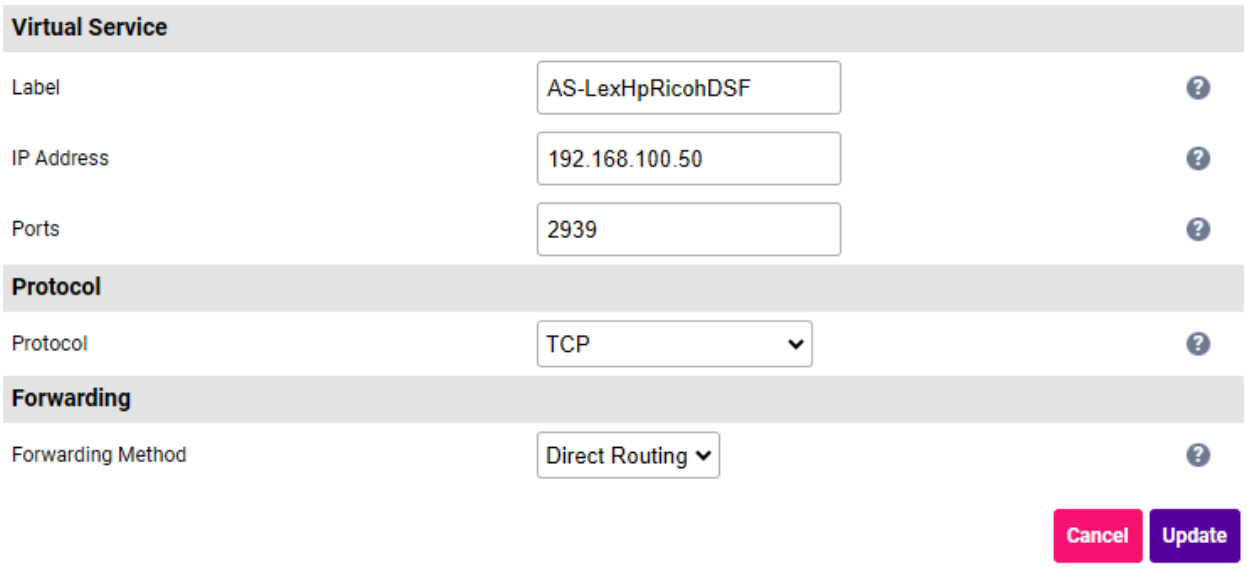
All shared printers and shared folders that have been configured on the Print Servers should be visible.

# 9. Configuring Load Balancing for Kofax Autostore

## 9.1. Appliance Configuration

### 9.1.1. Configure the Virtual Service (VIP)

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

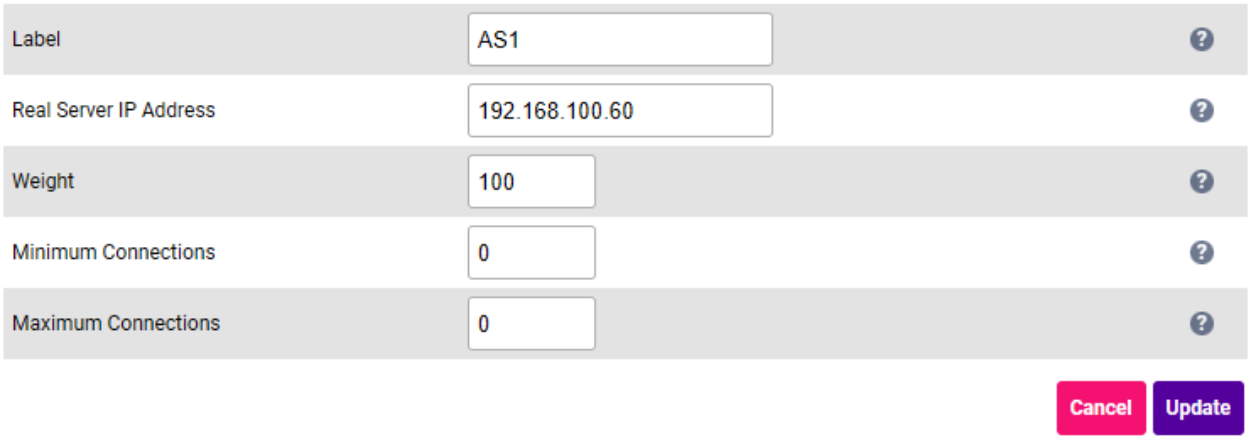


- Specify an appropriate *Label* for the Virtual Service, e.g. **AS-LexHpRicohDSF**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.100.50**.
- Set the *Ports* field according to your MFP vendor:
  - For Lexmark MFP / HP OXPd / Ricoh Desktop SF, specify **3233,3234**
  - For Ricoh ESA, specify **8084,9000**
  - for Ricoh SOP, specify **3350**
  - for Konica Minolta iOption, specify **3348,3281,13352,13353,13391**
  - If you're not sure of which ports are used by your MFP, an "all ports" VIP can be used as mentioned in Load Balancing Kofax AutoStore. For this, specify ***** (i.e. an asterisk).
- Ensure that the *Protocol* is set to **TCP**.
- Ensure that the *Forwarding Method* is set to **Direct Routing**.

3. Click **Update**.

### 9.1.2. Define the Associated Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.




- Specify an appropriate *Label* for the Real Server, e.g. **AS1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.100.60**.

2. Click **Update**.
3. Repeat these steps to add additional Autostore servers.

## 9.2. Kofax Autostore Configuration

### 9.2.1. Device Registration Service Configuration

Use Device Registration Service (DRS) to ensure that all required MFP clients are defined/installed.

### 9.2.2. Solve the ARP Problem

When using layer 4 DR mode, the "ARP Problem" must be solved on each AutoStore Server to enable DR mode to work correctly. The exact steps required depend on the particular operating system in use. To solve the ARP problem for Windows 2012 and later, please refer to Solving the ARP Problem in the appendix.

> **Note** For more details on the ARP problem, please refer to DR Mode Considerations.

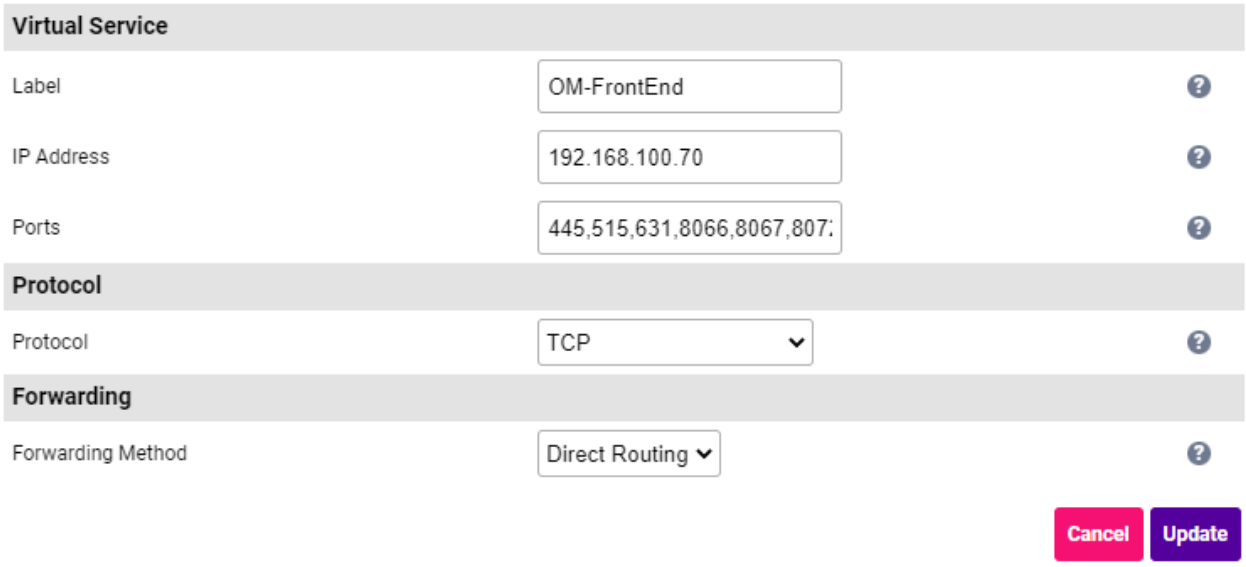
# 10. Configuring Load Balancing for Kofax Output Manager

## 10.1. Appliance Configuration

### 10.1.1. Front-End

#### Configure the Virtual Service (VIP)

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



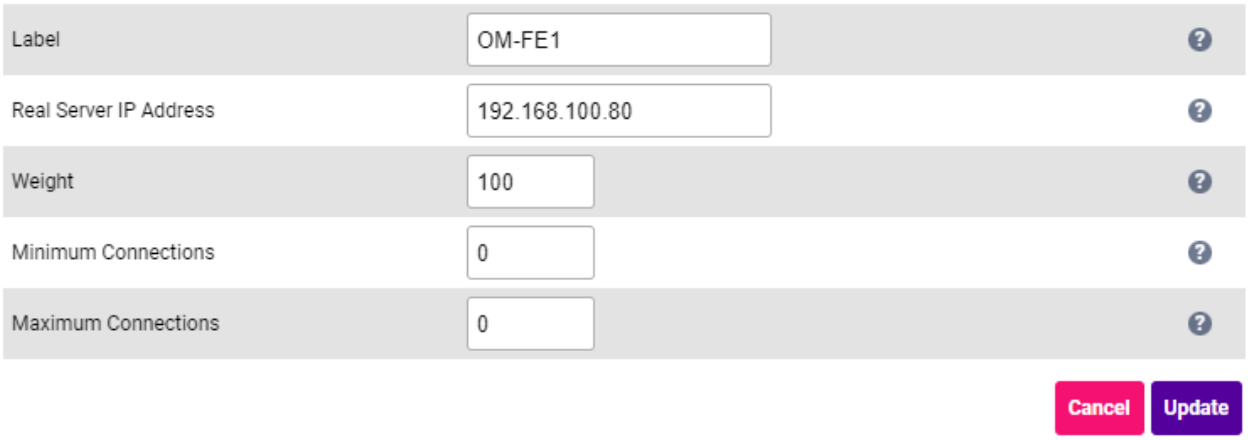

   - Specify an appropriate *Label* for the Virtual Service, e.g. **OM-FrontEnd**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.100.70**.
   - Set the *Ports* field to **445,515,631,8066,8067,8072,8076,9100**.
   - Ensure that the *Protocol* is set to **TCP**.
   - Ensure that the *Forwarding Method* is set to **Direct Routing**.
3. Click **Update**.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Persistence* section.
   - Clear the *Enable* checkbox to disable persistence.
6. Scroll to the *Health Checks* section.

- Set the *Check Port* to **8072**.
- Ensure that the *Protocol* is set to **TCP**.
- Ensure that the *Forwarding Method* is set to **Direct Routing**.

7. Click **Update**.

### Define the Associated Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.



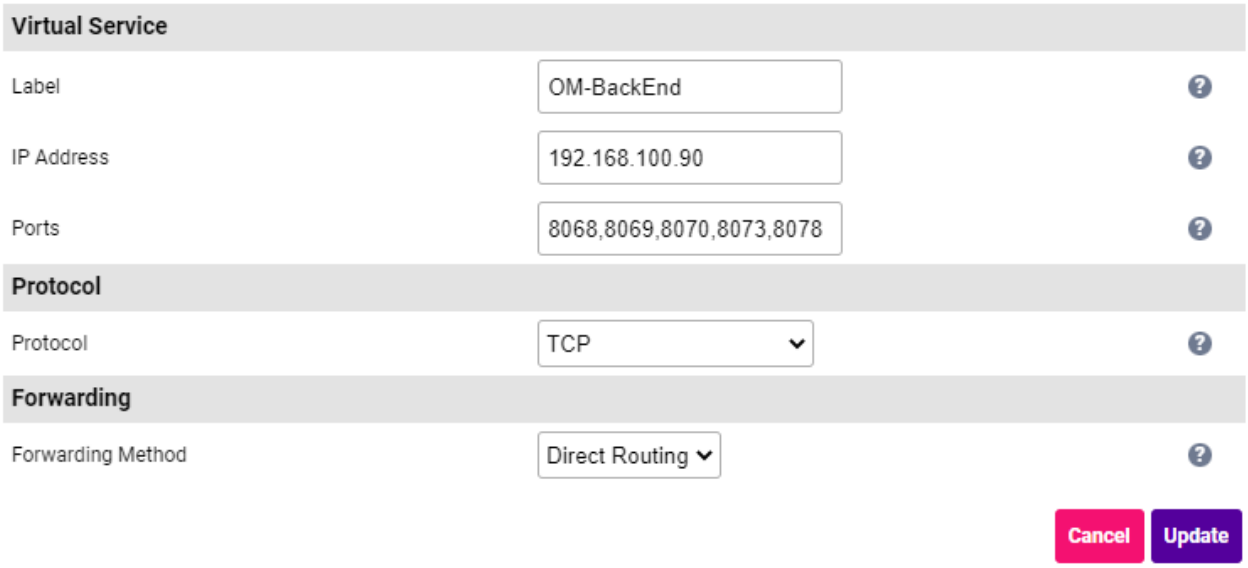

- Specify an appropriate *Label* for the Real Server, e.g. **OM-FE1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.100.80**.

2. Click **Update**.
3. Repeat these steps to add additional front-end servers.

## 10.1.2. Back-End

### Configure the Virtual Service (VIP)

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




- Specify an appropriate *Label* for the Virtual Service, e.g. **OM-BackEnd**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.100.90**.
- Set the *Ports* field to **8068,8069,8070,8073,8078**.
- Ensure that the *Protocol* is set to **TCP**.
- Ensure that the *Forwarding Method* is set to **Direct Routing**.

3. Click **Update**.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Persistence* section.
   - Clear the *Enable* checkbox to disable persistence.
6. Scroll to the *Health Checks* section.
   - Set the *Check Port* to **8078**.
7. Click **Update**.

## Define the Associated Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.


- Specify an appropriate *Label* for the Real Server, e.g. **OM-BE1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.100.100**.

2. Click **Update**.
3. Repeat these steps to add additional back-end servers.

## 10.2. Kofax Output Manager Configuration

### 10.2.1. Installing for High Availability

Output Manager must be installed For high availability to enable support for load balancing . For details, please refer to Output Manager in a high availability environment.

### 10.2.2. Solve the ARP Problem

When using layer 4 DR mode, the "ARP Problem" must be solved on each Output Manager Server to enable DR mode to work correctly. The exact steps required depend on the particular operating system in use. To solve the ARP problem for Windows 2012 and later, please refer to Solving the ARP Problem in the appendix.

> **Note** For more details on the ARP problem, please refer to DR Mode Considerations.

### 10.2.3. Device Registration Service Configuration

Use Device Registration Service (DRS) to ensure that all required MFP clients are defined/installed.

# 11. Testing & Verification

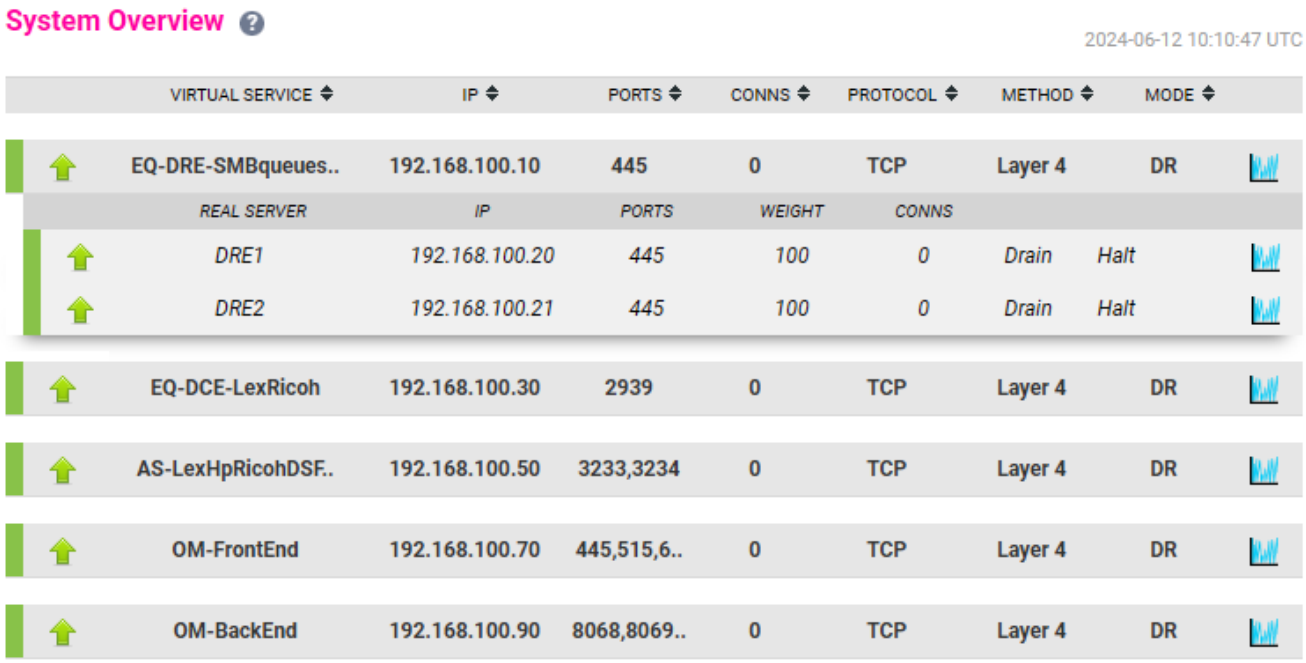
> **Note** For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

## 11.1. Testing ControlSuite

Once all configuration is complete on the load balancer, on the various ControlSuite servers and in the Device Registration Service, all functionality should be tested using the MFP.

## 11.2. Using System Overview

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




# 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:

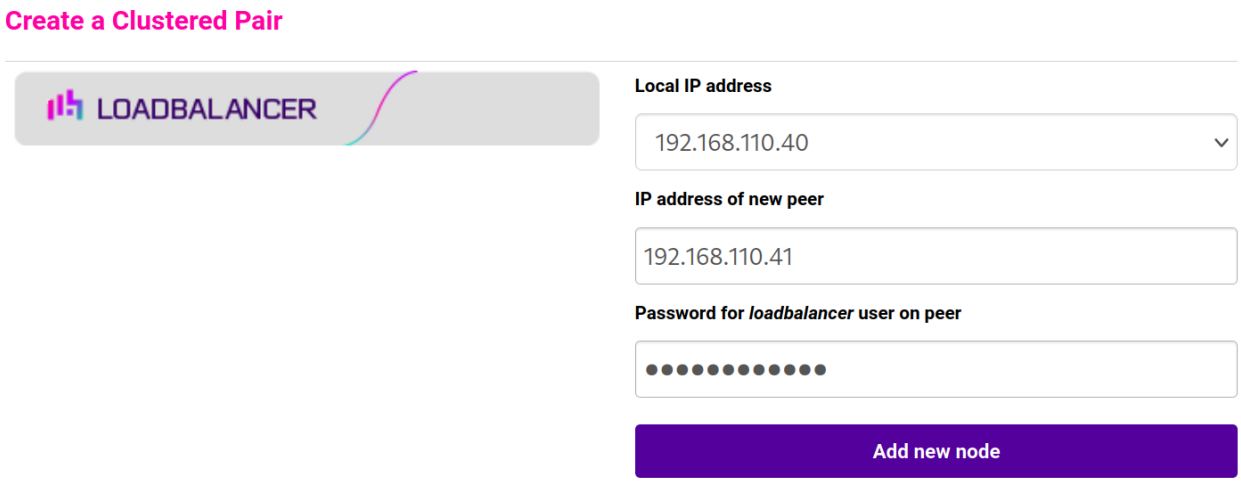
| WebUI Main Menu Option | Sub Menu Option | Description |
|---|---|---|
| Local Configuration | Hostname & DNS | Hostname and DNS settings |
| Local Configuration | Network Interface Configuration | Interface IP addresses, bonding configuration and VLANs |
| Local Configuration | Routing | Default gateways 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 | Fallback Page | Fallback page configuration |
| Maintenance | Firewall Script | Firewall (iptables) configuration |
| Maintenance | Firewall Lockdown Wizard | Appliance management lockdown settings |

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

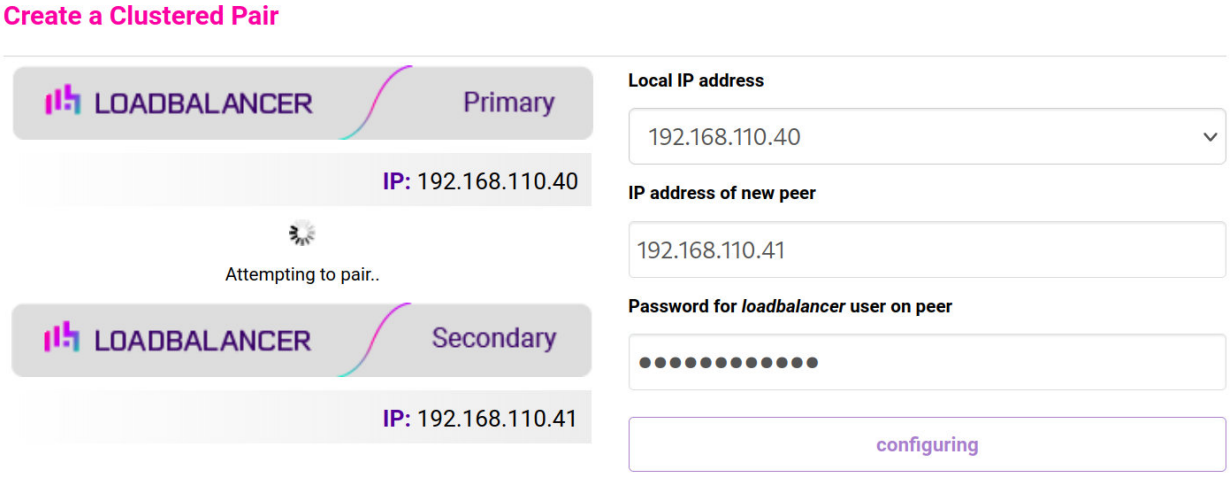
### 14.1.2. Configuring the HA Clustered Pair

> **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.

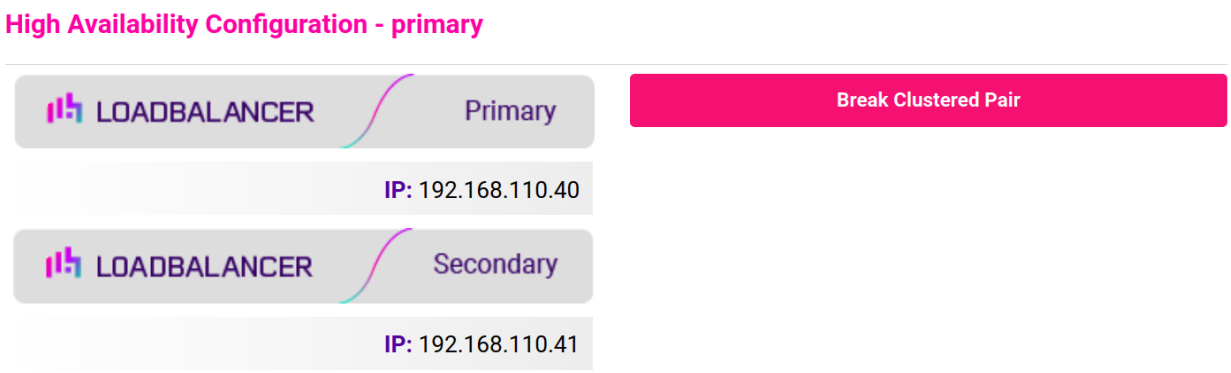
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.




3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown in the example above.
4. Click **Add new node**.
5. The pairing process now commences as shown below:




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




7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

> **Note** Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

> **Note** For more details on configuring HA with 2 appliances, please refer to Appliance Clustering for HA.

> **Note** For details on testing and verifying HA, please refer to Clustered Pair Diagnostics.

## 14.2. Solving the ARP Problem

### 14.2.1. Windows Server 2012 & Later

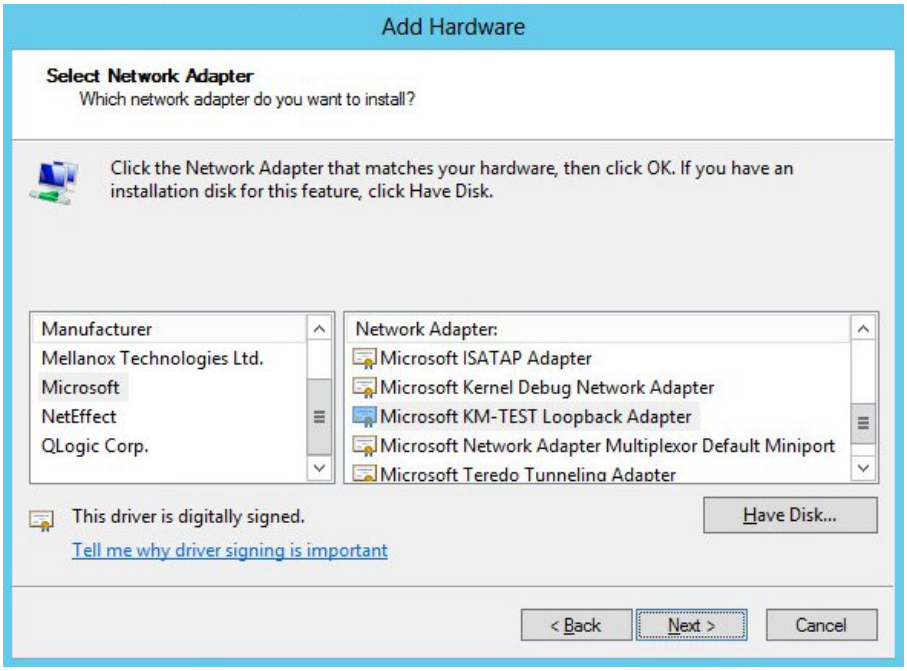
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables 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

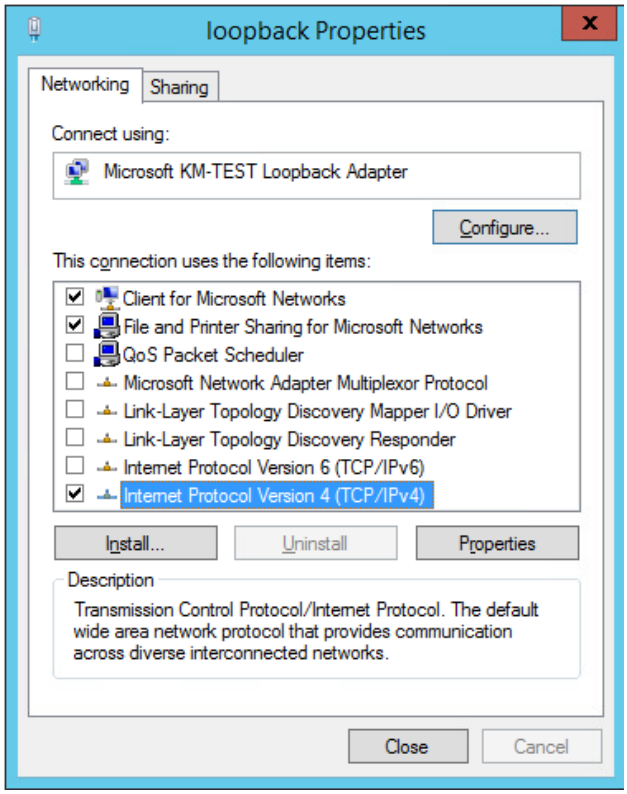
1. Open Control Panel and click **Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click the new Loopback Adapter and select **Properties**.

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

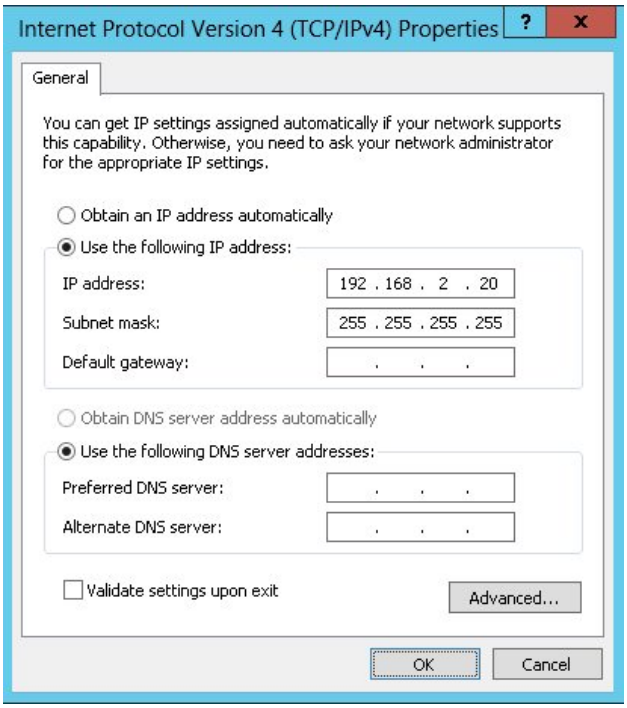
> **Important** When configuring the loopback adapter properties, make sure that **Client for Microsoft Networks** and **File & Printer Sharing for Microsoft Networks** is also checked as shown below.

### 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:



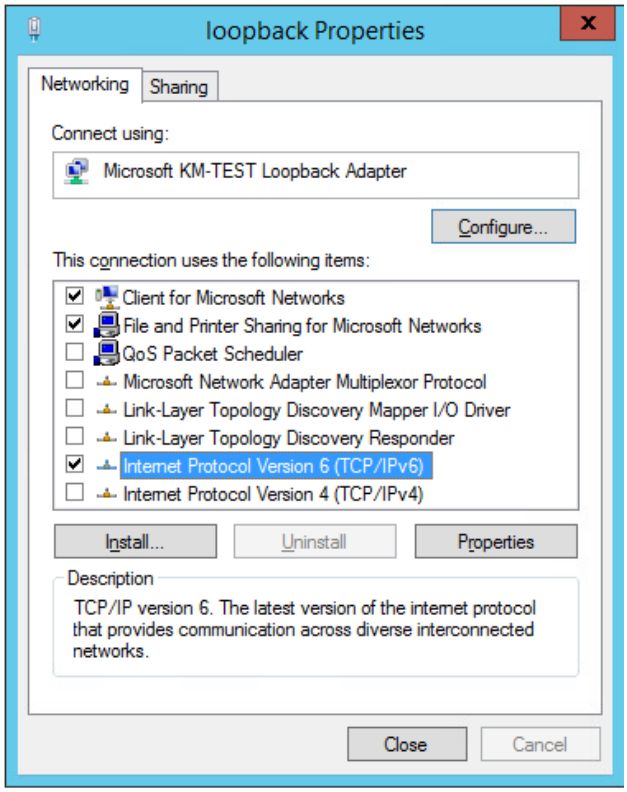

> **Note** **192.168.2.20** is an example, make sure you specify the correct VIP address.

> **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.

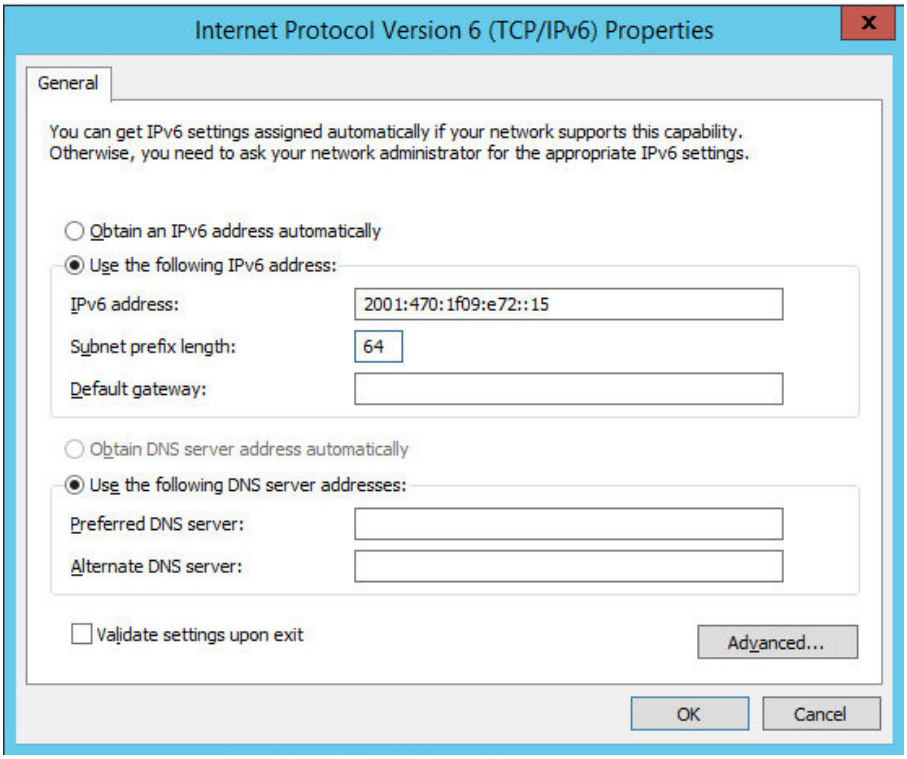
3. Click **OK** then click **Close** to save and apply the new settings.

### 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
```

# 15. Document Revision History

| Version | Date | Change | Reason for Change | Changed By |
|---|---|---|---|---|
| 1.0.0 | 1 October 2019 | Initial version | | AW |
| 1.0.1 | 6 November 2019 | Styling and layout | General styling updates | AH |
| 1.1.0 | 1 November 2021 | Converted the document to AsciiDoc | Move to new documentation system | AH, RJC, ZAC |
| 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<br><br>Added one level of section numbering<br><br>Reworded 'Further Documentation' section<br><br>Removed references to the colour of certain UI elements | Housekeeping across all documentation | AH |
| 1.1.3 | 2 February 2023 | Updated screenshots | Branding update | AH |
| 1.1.4 | 7 March 2023 | Removed conclusion section | Updates across all documentation | AH |
| 1.1.5 | 24 March 2023 | New document theme<br><br>Modified diagram colours | Branding update | AH |
| 2.0.0 | 3 July 2024 | Major document overhaul | Various additions, corrections and improvements to the document's content and structure | RJC |
| 2.0.1 | 15 January 2025 | Modified the "Load Balancer Deployment Methods" section to recommend layer 4 NAT mode then layer 7 SNAT mode if DR mode cannot be used. | | RJC |

LOADBALANCER

**Visit us:** www.loadbalancer.org

**Phone us:** +44 (0)330 380 1064

**Phone us:** +1 833 274 2566

**Email us:** info@loadbalancer.org

**Follow us:** @loadbalancer.org

## About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.