Load Balancing Kofax ControlSuite®

Version 1.2.0
# 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. Kofax ControlSuite ........................................... 4
4. Kofax ControlSuite .................................................. 4
5. Load Balancing Kofax ControlSuite ............................... 4
   5.1. Introduction and Overview of Different Modes .............. 4
   6.1. Layer 4 DR Mode .............................................. 5
6.2. Layer 4 NAT Mode ............................................... 6
   6.3. Layer 7 SNAT Mode ............................................ 8
7. Appliance Configuration for Kofax Equitrac – Using DR Mode .. 9
   7.1. Prerequisites .................................................. 9
   7.2. Overview of steps required ................................... 9
   7.3. Configuring the virtual service (VIP) ......................... 9
   7.4. Defining the Real Servers (RIPs) ............................ 10
8. Appliance Configuration for Microsoft Print Servers (Optional) – Using SNAT Mode 11
   8.1. Configuring the virtual service (VIP) ......................... 11
   8.2. Defining the Real Servers (RIPs) ............................ 11
9. Configuring Print Servers for Load Balancing .................... 12
   9.1. Registry Modifications ....................................... 12
       Microsoft Windows Server 2008 Specific Registry Change .... 13
   9.2. Configuring Name Resolution ................................ 13
       DNS Name Resolution (Windows 2000 & later) ................ 13
       NetBIOS Name Resolution (legacy Environments) .......... 14
   9.3. Finalising the Server Configuration ......................... 15
   9.4. Testing the load balanced print service ..................... 15
10. Kofax AutoStore .................................................... 15
11. Load Balancing Kofax AutoStore .................................. 16
   11.1. Load Balancing & HA Requirements ....................... 16
   11.2. Persistence (aka Server Affinity) ......................... 16
   11.3. Virtual Service (VIP) Requirements ....................... 16
   11.4. Port Requirements ......................................... 16
       Xerox EIP Connect .............................................. 16
       Konica Minolta ................................................. 17
       Ricoh ESA .................................................. 17
       Ricoh SOP .................................................. 17
       Other Vendors ............................................... 17
12. AutoStore Deployment Concept ................................... 17
13. Configuring Kofax AutoStore for Load Balancing ............... 18
   13.1. Device Registration Service Configuration ............... 18
   13.2. Layer 4 DR Mode – Solving the ARP Problem ............. 19
   14.1. Configuring the Virtual Service (VIP) ...................... 19
   14.2. Defining the Real Servers (RIPs) .......................... 20
15. Appliance Configuration for Kofax AutoStore – Using Layer 4 NAT Mode 21
   15.1. Configuring the Virtual Service (VIP) ...................... 21
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2. Defining the Real Servers (RIPs)</td>
<td>22</td>
</tr>
<tr>
<td>16. Testing &amp; Verification</td>
<td>23</td>
</tr>
<tr>
<td>16.1. Testing Using a Multi-function Device</td>
<td>23</td>
</tr>
<tr>
<td>16.2. Using the System Overview</td>
<td>23</td>
</tr>
<tr>
<td>17. Kofax Output Manager</td>
<td>24</td>
</tr>
<tr>
<td>18. Load Balancing Kofax Output Manager</td>
<td>24</td>
</tr>
<tr>
<td>18.1. Load Balancing &amp; HA Requirements</td>
<td>24</td>
</tr>
<tr>
<td>18.2. Persistence (aka Server Affinity)</td>
<td>24</td>
</tr>
<tr>
<td>18.3. Virtual Service (VIP) Requirements</td>
<td>25</td>
</tr>
<tr>
<td>18.4. Port Requirements</td>
<td>25</td>
</tr>
<tr>
<td>19. Output Manager Deployment Concept</td>
<td>25</td>
</tr>
<tr>
<td>20. Configuring Kofax Output Manager for Load Balancing</td>
<td>26</td>
</tr>
<tr>
<td>20.1. Registry Modifications</td>
<td>26</td>
</tr>
<tr>
<td>20.2. Configuring Name Resolution</td>
<td>26</td>
</tr>
<tr>
<td>20.3. Finalising the Configuration for Output Manager Back End Servers</td>
<td>26</td>
</tr>
<tr>
<td>20.4. Layer 4 DR Mode – Solving the ARP Problem</td>
<td>27</td>
</tr>
<tr>
<td>21.1. Configuring VIP 1 – Output Manager Front End</td>
<td>27</td>
</tr>
<tr>
<td>Configuring the Virtual Service (VIP)</td>
<td>27</td>
</tr>
<tr>
<td>Defining the Real Servers (RIPs)</td>
<td>28</td>
</tr>
<tr>
<td>21.2. Configuring VIP 2 – Output Manager Back End</td>
<td>29</td>
</tr>
<tr>
<td>Configuring the Virtual Service (VIP)</td>
<td>29</td>
</tr>
<tr>
<td>Defining the Real Servers (RIPs)</td>
<td>30</td>
</tr>
<tr>
<td>22. Appliance Configuration for Kofax Output Manager – Using Layer 7 SNAT Mode</td>
<td>31</td>
</tr>
<tr>
<td>22.1. Configuring VIP 1 – Output Manager Front End</td>
<td>31</td>
</tr>
<tr>
<td>Configuring the Virtual Service (VIP)</td>
<td>31</td>
</tr>
<tr>
<td>Defining the Real Servers (RIPs)</td>
<td>32</td>
</tr>
<tr>
<td>22.2. Configuring VIP 2 – Output Manager Back End</td>
<td>33</td>
</tr>
<tr>
<td>Configuring the Virtual Service (VIP)</td>
<td>33</td>
</tr>
<tr>
<td>Defining the Real Servers (RIPs)</td>
<td>34</td>
</tr>
<tr>
<td>22.3. Finalising the Configuration</td>
<td>35</td>
</tr>
<tr>
<td>23. Testing &amp; Verification</td>
<td>35</td>
</tr>
<tr>
<td>23.1. Testing the Load Balanced Print Service</td>
<td>35</td>
</tr>
<tr>
<td>23.2. Using the System Overview</td>
<td>35</td>
</tr>
<tr>
<td>24. Technical Support</td>
<td>36</td>
</tr>
<tr>
<td>25. Further Documentation</td>
<td>36</td>
</tr>
<tr>
<td>26. Appendix</td>
<td>37</td>
</tr>
<tr>
<td>26.1. Solving the ARP Problem</td>
<td>37</td>
</tr>
<tr>
<td>Windows Server 2012 &amp; Later</td>
<td>37</td>
</tr>
<tr>
<td>26.2. Configuring HA - Adding a Secondary Appliance</td>
<td>41</td>
</tr>
<tr>
<td>Non-Replicated Settings</td>
<td>42</td>
</tr>
<tr>
<td>Adding a Secondary Appliance - Create an HA Clustered Pair</td>
<td>42</td>
</tr>
<tr>
<td>26.3. Deploying Printers via Group Policy</td>
<td>44</td>
</tr>
<tr>
<td>27. Document Revision History</td>
<td>45</td>
</tr>
</tbody>
</table>
1. About this Guide

This guide details the steps required to configure a load balanced Kofax ControlSuite environment 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. Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.3.8 and later

The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If using an older software version, note that the screenshots presented here may not match the WebUI exactly.

3.2. Kofax ControlSuite

- All versions

4. Kofax ControlSuite

Kofax ControlSuite integrates a print management solution. Printing costs can be monitored, and can be reduced by forcing users to follow budget saving printing habits. Secure and regulations compliant printing is made possible by allowing users ‘pick up’ and print their secure documents in person at any printer. Flexible printing is achieved as users can print from anywhere, at anytime, and print from wherever they like. A capture application that captures, processes, and routes paper and electronic documents in a business environment. It lowers costs and improves operational efficiency for organizations of all sizes by automating document handling processes. With output management that gives organizations control of what, when, and how they produce and deliver information. Output Manager is designed to route documents through a centralized system into a single solution.

5. Load Balancing Kofax ControlSuite

5.1. Introduction and Overview of Different Modes

This guide details the configuration of a high availability ControlSuite deployment using a Loadbalancer.org appliance.
For a Kofax ControlSuite deployment, the preferred and default load balancer configuration uses Layer 4 DR Mode (Direct Routing, aka DSR / Direct Server Return) where possible. This is a very high performance solution that requires little change to your existing infrastructure. It is necessary to solve “the ARP problem” on the real print servers. This is a straightforward process, and is detailed in the section "Configuring Print Servers for Load Balancing".

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. However, we will only be using Layer 4 DR mode, Layer 4 NAT mode or Layer 7 SNAT modes in this guide.

6.1. Layer 4 DR Mode

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

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 you need to ensure that the Real Server (and the load balanced application) respond to both the Real Server’s own IP address and the VIP.
- The Real Servers should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as Solving the ARP problem. For more information please refer to DR Mode Considerations.
- On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP.
- The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work.
• The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet.

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

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

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 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.

  - Normally eth0 is used for the internal network and eth1 is used for the external network although this is optional. Any interface can be used for any purpose.

  - If the Real Servers require Internet access, Autonat 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.

© Copyright Loadbalancer.org • Documentation • Load Balancing Kofax ControlSuite®
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.

  - 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 Servers 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:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>VIP</th>
<th>Port</th>
<th>RIP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>10.0.0.20</td>
<td>80</td>
<td>192.168.1.50</td>
<td>80</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.x.x.x:34567</td>
<td>10.0.0.20:80</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.x.x.x:34567</td>
<td>192.168.1.50:80</td>
</tr>
</tbody>
</table>

3) Replies return to the load balancer as:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.50:80</td>
<td>x.x.x.x:34567</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.20:80</td>
<td>x.x.x.x:34567</td>
</tr>
</tbody>
</table>

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.
• Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.

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

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

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

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

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

7. Appliance Configuration for Kofax Equitrac – Using DR Mode

7.1. Prerequisites
A load balanced Kofax Equitrac environment requires the following:

• Microsoft Windows Server environment
• Installation of DCE server

7.2. Overview of steps required
Setting up a load balanced Kofax Equitrac environment can be summarised as follows:

• Create a virtual service (VIP) on the load balancer that listens on the required ports
• Associate the print servers to the virtual service, i.e. define them as ‘real servers’ (RIPs) for the VIP
• Install and configure the Kofax Equitrac DCE Windows print servers
• Configure registry settings on the print servers to enable them to be accessed via a shared name
• Configure name resolution related settings on the print servers
• Point users at the VIP to access the print server and the printer shares

7.3. 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. EQDCEHA.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.190.

4. Set the Ports as needed, depending on your MFP vendor:
   - For Lexmark and Ricoh, use port 2939
   - For HP OXPd, use ports 2939 and 7627

5. Click Update to create the virtual service.

6. Click Modify next to the newly created VIP.

7. Make sure that the Persistent checkbox is not selected.

8. Set the Check Port for server/service online to 2939.

9. Click Update.

7.4. 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. DCE1.

3. Set the Real Server IP Address field to the required IP address, e.g. 172.24.11.30.

4. Click Update.

5. Repeat these steps to add additional print servers as required.
8. Appliance Configuration for Microsoft Print Servers (Optional) – Using SNAT Mode

8.1. Configuring the virtual service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Virtual Services and click on Add a new Virtual Service.

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

3. Set the Virtual Service IP Address field to the required IP address, e.g. 172.24.11.10.

4. Set the Ports to 445.

5. Set the Layer 7 Protocol to TCP Mode.

6. Click Update.

8.2. Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Real Servers and click on Add a new Real Server next to the newly created VIP.

2. Define the Label for the real server as required, e.g. PS1.

3. Set the Real Server IP Address field to the required IP address, e.g. 172.24.11.40.

4. Leave the Real Server Port field blank.
5. Click **Update**.

6. Repeat these steps to add additional print servers as required.

7. Click on **Reload HAProxy** when prompted to do so in the "Commit changes" box that appears. This will apply the new changes and put the new virtual service and its associated virtual servers into use.

9. **Configuring Print Servers for Load Balancing**

The following steps should be carried out on each print server defined in the virtual service:

1. Join the server to the same domain as the client PCs.
2. Install the **Print and Document Service** role / **Print Server** service.
3. Install and share the printers (use exactly the same share names and permissions across all servers).
4. If DR mode is used, solve the "ARP problem" on each print server, to that DR mode will work. For detailed steps on solving the ARP problem for the various versions of Windows, please refer to **Solving the ARP Problem** for more information.

**Important**

When configuring the Loopback Adapter to solve the ARP Problem, the following options **must** also be checked (ticked):

- "Client for Microsoft Networks" & "File & Printer Sharing for Microsoft Networks"

### 9.1. Registry Modifications

To enable the print servers to be accessed via a shared name (**EQDCEHA** in the example virtual service in this guide), add the following registry entries to each print server:

- **Key:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
- **Value:** DisableLoopbackCheck
- **Type:** REG_DWORD
- **Data:** 1
In the example presented here, EQDCEHA is the name that will be used to access the load balanced print servers via the virtual service (VIP) created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address of the VIP as explained in the section below.

Microsoft Windows Server 2008 Specific Registry Change

If Microsoft Windows Server 2008 is used as the operating system for the printer servers, an additional registry entry change is required. The following registry entry should be changed from a DWORD to a QWORD:

- **Key:** HKLM\SYSTEM\CurrentControlSet\Control\Print\DNSOneWire
  - **Value:** DnsOnWire
  - **Type:** REG_QWORD
  - **Data:** 1

9.2. Configuring Name Resolution

For printer load balancing to work, either DNS or NetBIOS name resolution should be configured as detailed below.

DNS Name Resolution (Windows 2000 & later)

To configure DNS name resolution, the following steps should be completed:

1. NetBIOS over TCP/IP should be disabled on all interfaces of each print server, as shown:
2. A host name and corresponding “Host (A)” record for the virtual DCE that matches the virtual IP (VIP) address for the load balancer should be created.

When configuring printers to connect back to the highly available DCE, the DCE hostname / IP address should be the VIP address and not the individual DCE host name or IP address.

**NetBIOS Name Resolution (legacy Environments)**

To configure NetBIOS name resolution, the following steps should be completed:

1. NetBIOS over TCP/IP should be **disabled on the main NIC** and **left enabled on the Loopback adapter** on each print server.

2. Either a WINS server should be set up and all clients configured to use this, or pre-loaded entries in the LMHosts file of each client should be set up.

As shown in the flow chart in [this Technet article](#), for a default H-node client, NetBIOS name resolution occurs in the following order:

1. Local NetBIOS cache.
2. WINS server.
4. Local LMHosts file.

**Note**

Therefore, to avoid broadcast, LMHost entries must be declared as pre-loaded to ensure they are available in the local NetBIOS cache.
Configuring the LMHosts file
This is done by creating an entry like so:

```
EQDCEHA 192.168.100.10 #PRE
```

Entries with the #PRE directive are loaded into the cache on reboot, or can be forced using the command:

```
nbtstat -R
```

The following command can be used to view the cache and verify that the entry has been added:

```
nbtstat -c
```

9.3. Finalising the Server Configuration
To finalise the print server configuration changes, each print server must be rebooted.

9.4. Testing the load balanced print service
The load balanced print service can be tested, either by browsing to the virtual service IP address or the share name. In the example presented in this document, this would be done by going to

```
\192.168.85.190
```

or

```
\EQDCEHA
```

Any shared printers and shared folders that have been configured on the real print servers should be visible.

10. Kofax AutoStore
AutoStore is a server based middle-tier application that captures, processes, and routes paper and electronic documents in a business environment. It lowers costs and improves operational efficiency for organizations of all sizes by automating document handling processes.

AutoStore provides a flexible component-based server for capturing electronic and paper documents. Some of AutoStore's capabilities include:

- 'Capture components' to capture documents from scanners and multifunction devices, fax, email, smartphones and tablets, XML data streams, PC desktops, office applications, and network and FTP locations.
- 'Process components' to support functionalities to detect, read, extract, store, convert, classify, and index content in captured documents.
11. Load Balancing Kofax AutoStore

Note
It’s highly recommended that you have a working Kofax AutoStore environment first before implementing the load balancer.

11.1. Load Balancing & HA Requirements
In order to be successfully load balanced, a Kofax AutoStore deployment must feature the following components:

- Wide Area Network (WAN)
- Local Area Network (LAN)
- Firewall
- SQL Server
- Web Server
- Active Directory
- File Share

It is likely that a fully functional AutoStore deployment will already feature all of these components.

11.2. Persistence (aka Server Affinity)
MFDs from some vendors require source IP address persistence to be used for the AutoStore servers. This ensures that a particular client will connect to the same AutoStore server for the duration of the session.

MFDs from some vendors do not require session affinity at the load balancing layer.

Specific persistence settings for some of the most common vendors are described in the application configuration instructions later in this guide.

11.3. Virtual Service (VIP) Requirements
To provide load balancing and HA for AutoStore, a single VIP is required. The traffic that is load balanced and the ports that are used vary between vendors. Specific settings for some of the most common vendors are described in the application configuration instructions later in this guide.

11.4. Port Requirements
The following tables show the ports that are load balanced for four of the most common vendors:

Xerox EIP Connect
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>3241</td>
<td>TCP</td>
<td>Capture server port</td>
</tr>
</tbody>
</table>

**Konica Minolta**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>3348</td>
<td>TCP/HTTP</td>
<td>AutoStore Web Server</td>
</tr>
<tr>
<td>13351</td>
<td>TCP/HTTP</td>
<td>OpenAPI Application</td>
</tr>
<tr>
<td>13353</td>
<td>TCP/HTTPS</td>
<td>OpenAPI Authority</td>
</tr>
<tr>
<td>13391</td>
<td>TCP/HTTP</td>
<td>WebDAV Session</td>
</tr>
</tbody>
</table>

**Ricoh ESA**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>8084</td>
<td>TCP</td>
<td>Capture</td>
</tr>
<tr>
<td>8753</td>
<td>TCP</td>
<td>DRS</td>
</tr>
</tbody>
</table>

**Ricoh SOP**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>3350</td>
<td>TCP</td>
<td>Capture</td>
</tr>
<tr>
<td>8753</td>
<td>TCP</td>
<td>DRS</td>
</tr>
</tbody>
</table>

**Other Vendors**

If using a vendor that is not listed above, please follow the following hyperlink and refer to the port list for AutoStore provided by Kofax:

https://kofaximaging.custhelp.com/app/answers/detail/a_id/26545/~/default-ports-used-with-autostore-7-capture,-process,-and-route-components

The list includes the web application port / capture server port / web server port that should be used for a variety of vendors and services.

**12. AutoStore Deployment Concept**
VIPs = Virtual IP Addresses

13. Configuring Kofax AutoStore for Load Balancing

13.1. Device Registration Service Configuration

Kofax AutoStore needs to be configured via the Device Registration Service (DRS) so that it is highly available and can be load balanced.

The information for the load balanced virtual service needs to be entered into the DRS in the Add Application section.

- Set an appropriate name, e.g. xerox.
- Select the appropriate Application Type from the drop-down list, e.g. Xerox EIP Connect.
- Set the AutoStore Server Address to the virtual IP (VIP) address that will be used for the AutoStore virtual service.
- Set the Print Manager Address to the VIP used for the Output Manager backend.
- Set the Web Application Port as needed, depending on the MFD vendor:
  - For Xerox EIP Connect, use port 3241
  - For Konica Minolta, use port 3348
  - For Ricoh ESA, use port 8084
  - For Ricoh SOP, use port 3350
  - For other vendors, refer to Other Vendors
If any configuration changes are made to the AutoStore real servers they will need to be unregistered and then re-registered in the Device Registration Service for the configurations to be accepted.

Multi-function devices (MFDs) should be in the same group/folder in the Device Registration Service so that they inherit the same configuration.

13.2. Layer 4 DR Mode – Solving the ARP Problem

If using layer 4 DR mode, the 'ARP problem' must be solved on each real server for DR mode to work. For detailed steps on solving the ARP problem for Windows, please refer to Solving the ARP Problem for more information.

For a detailed explanation of DR mode and the nature of the ARP problem, please refer to Layer 4 DR Mode.


14.1. 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. AutoStore-KonicaMinolta.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.10.

4. Set the Ports field as needed, as a comma separated list, depending on the MFD vendor:
   - For Xerox EIP Connect, use port 3241
   - For Konica Minolta, use ports 3348, 13351, 13353, and 13391
   - For Ricoh ESA, use ports 8084 and 8753
   - For Ricoh SOP, use ports 3350 and 8753
   - For other vendors, refer to Other Vendors

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**

- **Label**: AutoStore-KonicaMinolta
- **IP Address**: 192.168.85.10
- **Ports**: 3348,13351,13353,13391
- **Protocol**: TCP
- **Forwarding Method**: Direct Routing

---

8. Click **Modify** next to the newly created VIP.

9. Set **Balance Mode** to **Weighted Round Robin**.

10. Set the persistence settings as required, depending on the MFD vendor:
   - For Xerox EIP Connect and Konica Minolta:
     - Make sure that the **Persistent** checkbox is checked
     - Set the **Timeout** value to **300** (the units are seconds)
   - For Ricoh ESA and Ricoh SOP, make sure that the **Persistent** checkbox is not selected

11. Click **Update**.

---

**Layer 4 - Modify Virtual Service**

---

14.2. 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. **AutoStore1**.

3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.20**.

4. Click **Update**.

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

---

15. Appliance Configuration for Kofax AutoStore – Using Layer 4 NAT Mode

### 15.1. 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. Enter an appropriate name for the VIP in the **Label** field, e.g. **AutoStore-RicohESA**.

3. Set the **Virtual Service IP** address field to the required IP address, e.g. **192.168.85.10**.

4. Set the **Virtual Service Ports** field as needed, as a comma separated list, depending on the MFD vendor:
   - For Xerox EIP Connect, use port **3241**
   - For Konica Minolta, use ports **3348, 13351, 13353, and 13391**
   - For Ricoh ESA, use ports **8084 and 8753**
   - For Ricoh SOP, use ports **3350 and 8753**
   - For other vendors, refer to **Other Vendors**

5. Set the **Forwarding Method** to **NAT**.
6. Click **Update** to create the virtual service.

7. Click **Modify** next to the newly created VIP.

8. Set **Balance Mode** to **Weighted Round Robin**.

9. Set the **Persistence Mode** settings as required, depending on the MFD vendor:
   - For Xerox EIP Connect and Konica Minolta:
     - Set **Persistence Mode** to **Source IP** persistence
     - Set the **Timeout** value to **300** (the units are seconds)
   - For Ricoh ESA and Ricoh SOP, set **Persistence Mode** to **None**

10. Click **Update**.

### 15.2. 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. Enter an appropriate name for the server in the **Label** field, e.g. **AutoStore1**.

3. Change the **Real Server IP Address** field to the required IP address, e.g. **172.24.11.20**.

4. Leave the **Real Server Port** field empty.

5. Click **Update**.

6. Repeat these steps to add additional AutoStore servers as required.

### Layer 4 Add a new Real Server - AutoStore-RicohESA

<table>
<thead>
<tr>
<th>Label</th>
<th>AutoStore1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>172.24.11.20</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

**Note**

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

### 16. Testing & Verification

#### 16.1. Testing Using a Multi-function Device

Once all configuration is complete on the AutoStore servers, in the Device Registration Service, and on the load balancer, it is possible to test the new load balanced service using a multi-function device.

1. Authenticate at a configured multi-function device.
2. Press the Kofax button and then select a scan template, for example to scan to home or scan to e-mail.
3. Set the scan options as appropriate, and complete a test scan.
4. AutoStore should recognise the user authenticated at the multi-function device and then route the test scan as requested. Verify that the test scan arrives at its intended destination.

#### 16.2. Using the System Overview

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

Kofax Output Manager gives organizations control of what, when, and how they produce and deliver information. Output Manager is designed to route documents through a centralized system.

Kofax Output Manager consolidates input from multiple platforms and applications. It centrally manages resources and documents, and provides end-to-end tracking and reporting. Although documents traditionally travel directly from origin to destination, there are considerable benefits to routing them through a centralized system. Output Manager is therefore built around these main concepts:

- Maximize the number of sources from which you can receive documents
- Provide greater control over documents than can be found in other products
- Manage and expand the number of document destinations
- Insure the security and integrity of documents throughout the send/receive cycle
- Produce a completely integrated audit trail and accounting functionality in order to monitor and control your costs
- Supply the tools necessary to convert document formats based upon the final destination
- Provide an observable process to a variety of audiences including administrators, print operators, end users, and management

18. Load Balancing Kofax Output Manager

18.1. Load Balancing & HA Requirements

The Output Manager components in a high availability environment require the following prerequisites to be installed and configured as per the Kofax Output Manager Installation Guide:

- Output Manager Core Server
- Output Manager Distributed Server
- Output Manager Web Server
- Output Manager Console
- Output Manager File Store
- Output Manager Web Client

18.2. Persistence (aka Server Affinity)

Kofax Output Manager does not require session affinity at the load balancing layer, as the back end uses an SQL database to handle session state.
18.3. Virtual Service (VIP) Requirements

To provide load balancing and HA for Product Name, the following VIPs are required:

- Output Manager Front End
- Output Manager Back End (using either HTTP or HTTPS)

18.4. Port Requirements

The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>445</td>
<td>TCP/SMB</td>
<td>Output Manager front end</td>
</tr>
<tr>
<td>8068</td>
<td>TCP/HTTP</td>
<td>Output Manager back end over HTTP</td>
</tr>
<tr>
<td>8069</td>
<td>TCP/HTTPS</td>
<td>Output Manager back end over HTTPS</td>
</tr>
</tbody>
</table>

19. Output Manager Deployment Concept

VIPs = Virtual IP Addresses
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.

20. Configuring Kofax Output Manager for Load Balancing

20.1. Registry Modifications
For the print servers that are going to be load balanced, to enable them to be accessed via a shared name (XeroxPrintService is the example used in this guide), add the following registry entries to each print server:

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: XeroxPrintService

In the example presented here, XeroxPrintService is the name that will be used to access the load balanced print servers via the virtual service (VIP) created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address of the VIP.

20.2. Configuring Name Resolution
For printer load balancing to work, DNS name resolution should be configured. A host name and corresponding 'Host (A)' record for the virtual service should be created, and should match the virtual IP (VIP) address defined on the load balancer.

20.3. Finalising the Configuration for Output Manager Back End Servers
To finalise the print server configuration changes, each print server must be rebooted.

In order to load balance Output Manager back end servers, Output Manager needs to be configured for high availability within the Output Manager Server Configuration Utility. This allows the user to select the Use HA check box where the user will be able to enter the associated load balancer virtual server IP address (VIP) or the DNS alias for the VIP created.

For further details on how to configure Output Manager back end servers please refer to page 37 of the Output Manager ControlSuite® documentation.
Multi-function devices (MFDs) should be in the same group/folder in the Device Registration Service so that they inherit the same configuration.

20.4. Layer 4 DR Mode – Solving the ARP Problem

If using layer 4 DR mode, the ‘ARP problem’ must be solved on each real server for DR mode to work. For detailed steps on solving the ARP problem for Windows, please refer to Solving the ARP Problem for more information.

For a detailed explanation of DR mode and the nature of the ARP problem, please refer to Layer 4 DR Mode.


When deploying Kofax Output Manager, two virtual services must be configured: a virtual service for the Output Manager front end, and a virtual service for the Output Manager back end.

21.1. Configuring VIP 1 – Output Manager Front End

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. OM-FrontEnd.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.50.
4. Set the Ports to 445.
5. Leave the Protocol set to TCP.
7. Click Update to create the virtual service.
8. Click **Modify** next to the newly created VIP.
9. Set **Balance Mode** to **Weighted Round Robin**.
10. Make sure that the **Persistent** checkbox is not selected.
11. Set the **Health Checks Check Type** to **Connect to port**.
12. Set the **Check Port** to **445**.
13. Click **Update**.

### Layer 4 - Modify Virtual Service

<table>
<thead>
<tr>
<th>Label</th>
<th>OM-FrontEnd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td>192.168.85.50</td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>445</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
<tr>
<td>Balance Mode</td>
<td>Weighted Round Robin</td>
</tr>
<tr>
<td>Persistent</td>
<td></td>
</tr>
<tr>
<td>Health Checks</td>
<td></td>
</tr>
<tr>
<td>Check Type</td>
<td>Connect to port</td>
</tr>
<tr>
<td>Check Port</td>
<td>445</td>
</tr>
</tbody>
</table>

### 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. **OM-FrontEnd-Srv1**.
3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.100.200**.
4. Click **Update**.
5. Repeat these steps to add additional real servers as required.
21.2. Configuring VIP 2 – Output Manager Back End

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. OM-BackEnd.

3. Set the **Virtual Service IP Address** field to the required IP address, e.g. 192.168.85.60.

4. Set the **Ports** field as required, based on your setup:
   - If only HTTP traffic will be passed to the back end, set the **Ports** field to 8068
   - If only HTTPS traffic will be passed to the back end, set the **Ports** field to 8069

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

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

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

8. Click **Modify** next to the newly created VIP.

9. Set **Balance Mode** to Weighted Round Robin.
10. Make sure that the **Persistent** checkbox is not selected.

11. Set the **Health Checks Check Type** to **Connect to port**.

12. Set the **Check Port** to the same port defined under **Virtual Service Ports**, i.e. either **8068** or **8069**.

13. Click **Update**.

---

**Layer 4 – Modify Virtual Service**

<table>
<thead>
<tr>
<th>Label</th>
<th>OM-BackEnd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td>192.168.85.60</td>
</tr>
<tr>
<td>Ports</td>
<td>8069</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
<tr>
<td>Balance Mode</td>
<td>Weighted Round Robin</td>
</tr>
<tr>
<td>Persistent</td>
<td></td>
</tr>
<tr>
<td>Health Checks</td>
<td>Connect to port</td>
</tr>
<tr>
<td>Check Port</td>
<td>8069</td>
</tr>
</tbody>
</table>

**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. **OM-BackEnd-Srv1**.

3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.210**.

4. Click **Update**.

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

---

**Layer 4 Add a new Real Server – OM-BackEnd**

<table>
<thead>
<tr>
<th>Label</th>
<th>OM-BackEnd-Srv1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.85.210</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>
22. Appliance Configuration for Kofax Output Manager – Using Layer 7 SNAT Mode

When deploying Kofax Output Manager, two virtual services must be configured: a virtual service for the Output Manager front end, and a virtual service for the Output Manager back end.

22.1. Configuring VIP 1 – Output Manager Front End

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. OM-FrontEnd.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.50.
4. Set the Ports field to 445.
5. Set the Layer 7 Protocol to TCP Mode.
6. Click Update to create the virtual service.

7. Click Modify next to the newly created VIP.
8. Set Balance Mode to Weighted Round Robin.
9. Set Persistence Mode to None.
10. Set Health Checks to Connect to port.
11. Set Check Port to the "Port" value, e.g. 445.
12. 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. *OM-FrontEnd-Srv1*.

3. Set the *Real Server IP Address* field to the required IP address, e.g. *192.168.100.200*.

4. Set the *Real Server Port* field to *445*.

5. Click *Update*.

6. Repeat these steps to add additional real servers as required.
### 22.2. Configuring VIP 2 – Output Manager Back End

#### 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. **OM-BackEnd**.

3. Set the **Virtual Service IP Address** field to the required IP address, e.g. **192.168.85.60**.

4. Set the **Ports** field as required, based on your setup:
   - If only HTTP traffic will be passed to the back end, set the **Ports** field to **8068**
   - If only HTTPS traffic will be passed to the back end, set the **Ports** field to **8069**

5. Set the **Layer 7 Protocol** to **TCP Mode**.

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

7. Click **Modify** next to the newly created VIP.

8. Set **Balance Mode** to **Weighted Round Robin**.

9. Set **Persistence Mode** to **None**.
10. Set **Health Checks** to **Connect to port**.

11. Set the **Check Port** to the same port defined under **Virtual Service Ports**, i.e. either **8068** or **8069**.

12. Click **Update**.

### Layer 7 - Modify Virtual Service

<table>
<thead>
<tr>
<th>Manual Configuration</th>
<th><img src="help.png" alt="Help" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>OM-BackEnd</td>
</tr>
<tr>
<td>Virtual Service</td>
<td><img src="help.png" alt="Help" /></td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.85.60</td>
</tr>
<tr>
<td>Ports</td>
<td>8069</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td><img src="help.png" alt="Help" /></td>
</tr>
<tr>
<td>TCP Keep-alive</td>
<td><img src="help.png" alt="Help" /></td>
</tr>
<tr>
<td>Balance Mode</td>
<td>Weighted Round Robin</td>
</tr>
<tr>
<td>Persistence Mode</td>
<td>None</td>
</tr>
<tr>
<td>Feedback Method</td>
<td>None</td>
</tr>
<tr>
<td>Fallback Server</td>
<td><img src="help.png" alt="Help" /></td>
</tr>
<tr>
<td>IP Address</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>Port</td>
<td>9081</td>
</tr>
<tr>
<td>Fallback Persistence</td>
<td><img src="help.png" alt="Help" /></td>
</tr>
<tr>
<td>Health Checks</td>
<td><img src="help.png" alt="Help" /></td>
</tr>
<tr>
<td>Check Port</td>
<td>8069</td>
</tr>
</tbody>
</table>

### 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. **OM-BackEnd-Srv1**.

3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.210**.

4. Leave the **Real Server Port** field empty.

5. Click **Update**.

6. Repeat these steps to add additional real servers as required.
22.3. 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**.

23. Testing & Verification

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

23.1. Testing the Load Balanced Print Service

The load balanced print service can be tested, either by browsing to the virtual service IP address or the share name, so for example

\192.168.85.190

or

\XeroxPrintService

Any shared printers and shared folders that have been configured on the real print servers should be visible.

It is also possible to test by using an Active Directory user and computers to set up a Group Policy Object (GPO) pointing to the Output Manager front end VIP. For more details on how to do this, refer to **Deploying Printers via Group Policy** for more information.

23.2. Using the System Overview

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

### System Overview

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th>IP</th>
<th>Ports</th>
<th>Conns</th>
<th>Protocol</th>
<th>Method</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>OM-FrontEnd</td>
<td>192.168.85.50</td>
<td>445</td>
<td>0</td>
<td>TCP</td>
<td>Layer 4</td>
<td>DR</td>
</tr>
<tr>
<td>OM-FrontEnd-Srv1</td>
<td>192.168.85.200</td>
<td>445</td>
<td>100</td>
<td>TCP</td>
<td>Drain</td>
<td>Halt</td>
</tr>
<tr>
<td>OM-FrontEnd-Srv2</td>
<td>192.168.85.201</td>
<td>445</td>
<td>100</td>
<td>TCP</td>
<td>Drain</td>
<td>Halt</td>
</tr>
<tr>
<td>OM-BackEnd</td>
<td>192.168.85.60</td>
<td>8069</td>
<td>0</td>
<td>TCP</td>
<td>Layer 4</td>
<td>DR</td>
</tr>
</tbody>
</table>

### 24. 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.

### 25. Further Documentation

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

26.1. Solving the ARP Problem

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.

Note

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

In addition, steps must be taken to set the strong/weak host behavior on each Real Server. This is used to either prevent or allow interfaces to receive packets destined for a different interface on the same server.

Important

The following 3 steps must be completed on each Real Server.

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:

![IPv4 Addresses Configuration](image)

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

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:

![Internet Protocol Version 6 (TCP/IPv6) Properties](image)

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

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

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

Either Network Shell (**netsh**) commands or PowerShell cmdlets can be used to set the required strong/weak host behavior.

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:

![Network Connections](image)

- **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:

```bash
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:

```bash
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:

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

For IPv6 Addresses:

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

### 26.2. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution.

We recommend that the Primary appliance is configured first and then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically replicated to the Secondary over the network using SSH/SCP.

**Note**

For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified - one for the VIP when it's active on the Primary and one for the VIP when it's active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.
The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

**Non-Replicated Settings**

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>

**Important**

Make sure that if these settings/updates have been configured on the Primary appliance, they’re also configured on the Secondary appliance.

**Adding a Secondary Appliance - Create an HA Clustered Pair**

**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.
26.3. Deploying Printers via Group Policy

It is possible to deploy a printer using a Group Policy, by following these steps:

1. Ensure that the load balanced print server name (e.g. XeroxPrintService) is resolvable by DNS or NetBIOS, as explained in Configuring Name Resolution.

2. On your print server, open: Administrative Tools > Printer Management.

3. Right-click Print Servers and enter the name for your load balanced print server (e.g. XeroxPrintService) and click OK.

4. Expand the Printers section.

5. Right click the printer you want to deploy, and click Deploy with Group Policy.

6. Select the relevant GPO and configure the remaining settings according to your requirements.
## 27. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9.6</td>
<td>1 October 2019</td>
<td>Initial version</td>
<td></td>
<td>AW</td>
</tr>
<tr>
<td>1.0.0</td>
<td>6 November 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>3 September 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td>1.1.0</td>
<td>1 November 2021</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</td>
</tr>
<tr>
<td>1.1.1</td>
<td>28 September 2022</td>
<td>Updated layer 7 VIP and RIP creation screenshots</td>
<td>Reflect changes in the web user interface</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.2</td>
<td>5 January 2023</td>
<td>Combined software version information into one section</td>
<td>Housekeeping across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added one level of section numbering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reworded 'Further Documentation' section</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Removed references to the colour of certain UI elements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.3</td>
<td>2 February 2023</td>
<td>Updated screenshots</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.4</td>
<td>7 March 2023</td>
<td>Removed conclusion section</td>
<td>Updates across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td>1.2.0</td>
<td>24 March 2023</td>
<td>New document theme</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified diagram colours</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About Loadbalancer.org

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

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