Load Balancing Kofax Output Manager
Version 1.2.0
# Table of Contents

1. About this Guide ................................................................. 4
2. Loadbalancer.org Appliances Supported ............................... 4
3. Loadbalancer.org Software Versions Supported ......................... 4
4. Kofax Output Manager Software Versions Supported ................ 4
5. Kofax Output Manager .......................................................... 4
6. Load Balancing Kofax Output Manager ..................................... 5
   Load Balancing & HA Requirements ...................................... 5
   Persistence (aka Server Affinity) .......................................... 5
   Virtual Service (VIP) Requirements ..................................... 5
   Port Requirements .......................................................... 5
7. Deployment Concept ............................................................ 5
8. Load Balancer Deployment Methods ....................................... 6
   Layer 4 DR Mode .................................................................. 6
   Layer 7 SNAT Mode ........................................................... 7
   Our Recommendation .......................................................... 8
9. Configuring Kofax Output Manager for Load Balancing ................. 8
   Registry Modifications ....................................................... 8
   Configuring Name Resolution .............................................. 9
   Finalising the Configuration for Output Manager Back End Servers .. 9
   Layer 4 DR Mode – Solving the ARP Problem .......................... 9
10. Loadbalancer.org Appliance – the Basics ................................. 9
    Virtual Appliance ............................................................. 10
    Initial Network Configuration ............................................. 10
    Accessing the WebUI ........................................................ 10
    Main Menu Options .......................................................... 11
    HA Clustered Pair Configuration ........................................ 12
11. Appliance Configuration for Kofax Output Manager – Using Layer 4 DR Mode 12
    Configuring VIP 1 – Output Manager Front End ....................... 12
    Configuring the Virtual Service (VIP) ................................... 12
    Defining the Real Servers (RIPs) ....................................... 13
    Configuring VIP 2 – Output Manager Back End ....................... 13
    Configuring the Virtual Service (VIP) ................................... 13
    Defining the Real Servers (RIPs) ....................................... 15
12. Appliance Configuration for Kofax Output Manager – Using Layer 7 SNAT Mode 15
    Configuring VIP 1 – Output Manager Front End ....................... 15
    Configuring the Virtual Service (VIP) ................................... 15
    Defining the Real Servers (RIPs) ....................................... 16
    Configuring VIP 2 – Output Manager Back End ....................... 17
    Configuring the Virtual Service (VIP) ................................... 17
    Defining the Real Servers (RIPs) ....................................... 18
    Finalising the Configuration ................................................ 19
13. Testing & Verification ............................................................ 19
    Testing the Load Balanced Print Service .................................. 19
    Using System Overview ...................................................... 19
14. Technical Support ............................................................... 20
15. Further Documentation ........................................................ 20
16. Conclusion ......................................................................... 20
17. Appendix .......................................................................... 21
    Solving the ARP Problem ..................................................... 21
1. About this Guide

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

- V8.4.1 and later

Note: 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.

4. Kofax Output Manager Software Versions Supported

- Kofax Output Manager – version 4.0 SP1 and later

5. 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
- Ensure 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
6. Load Balancing Kofax Output Manager

Note: It's highly recommended that you have a working Kofax Output Manager environment first before implementing the load balancer.

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

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.

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)

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>

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

8. 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 Output Manager, layer 4 DR mode and layer 7 SNAT mode are recommended. These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode please refer to Appliance Configuration for Kofax Output Manager – Using Layer 4 DR Mode and for configuring using layer 7 SNAT mode refer to Appliance Configuration for Kofax Output Manager – Using Layer 7 SNAT Mode.

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 N-Path.
- 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.

### 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 additional configuration changes to the load balanced Real Servers.

Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 \(\rightarrow\) 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.

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

If DR mode cannot be used, for example if it is not possible to make changes to the real servers, or if the real servers are located in remote routed networks, then layer 7 SNAT mode is recommended.

9. Configuring Kofax Output Manager for Load Balancing

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
```

**Note**

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.

**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.

**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 Installation Guide Version 4.0 SP2'.

**Note**

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

**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](#).

10. Loadbalancer.org Appliance – the Basics
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.

Initial Network Configuration

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

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

Accessing the WebUI

The WebUI is accessed using a web browser. By default, user authentication is based on local Apache .htaccess files. User administration tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.

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

Note: If required, users can also be authenticated against LDAP, LDAPS, Active Directory or Radius. For more information please refer to External Authentication.

1. Using a browser, access the WebUI using the following URL:


2. Log in to the WebUI:

   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:
Note: The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.

3. You’ll be asked if you want to run the Setup Wizard. If you click **Accept** the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simple click **Dismiss**.

**Main Menu Options**

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

11. Appliance Configuration for Kofax Output Manager – Using 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.

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.


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>192.168.50.50</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>False</td>
</tr>
<tr>
<td>Health Checks</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.

---

**Layer 4 Add a new Real Server - OM-FrontEnd**

<table>
<thead>
<tr>
<th>Label</th>
<th>OM-FrontEnd-Srv1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.100.200</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>

---

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

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

12. 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.

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. Under the **Health Checks** section click **Advanced** to expand the menu.
11. Set **Health Checks** to **Connect to port**.
12. Set **Check Port** to the "Port" value, e.g. **445**.
13. 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.

```
Layer 7 Add a new Real Server - OM-FrontEnd

<table>
<thead>
<tr>
<th>Label</th>
<th>OM-FrontEnd-Srv1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.100.200</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>445</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>
```

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.

```
Layer 7 - Add a new Virtual Service

<table>
<thead>
<tr>
<th>Label</th>
<th>OM-BackEnd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service 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>TCP Mode</td>
</tr>
</tbody>
</table>
```

© Copyright Loadbalancer.org • Documentation • Load Balancing Kofax Output Manager
7. Click **Modify** next to the newly created VIP.
8. Set **Balance Mode** to **Weighted Round Robin**.
9. Set **Persistence Mode** to **None**.
10. Under the **Health Checks** section click **Advanced** to expand the menu.
11. Set **Health Checks** 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**.

---

**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. 192.168.85.201.
4. Leave the **Real Server Port** field empty.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.
Finalizing the Configuration
To apply the new settings, HAProxy must be reloaded. This can be done using the button in the blue 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.

13. Testing & Verification

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

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

\10.10.10.190

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.

Using 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.
14. 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.

15. Further Documentation

16. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Kofax Output Manager environments.
17. Appendix

Solving the ARP Problem

When using Layer 4 DR mode, the ARP problem must be solved. This involves configuring each Real Server to be able to receive traffic destined for the VIP, and ensuring that each Real Server does not respond to ARP requests for the VIP address – only the load balancer should do this. The steps below are for Windows 2012 and later.

Windows Server 2012 & Later

Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter. The IP address allocated to the Loopback Adapter must be the same as the Virtual Service (VIP) address. If the Real Server is included in multiple DR mode VIPs, additional IP addresses can be added to the Loopback Adapter that correspond to each VIP. In addition, steps must be taken to set the strong/weak host behavior which is used to either block or allow interfaces to receive packets destined for a different interface on the same server.

Step 1 of 3: Install the Microsoft Loopback Adapter

1. Click Start, then run hdwwiz to start the Hardware Installation Wizard.
2. When 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**.

4. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:

   ![Loopback Properties](image)

   **Note**

   Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred.

   **Important**

   When configuring the Loopback Adapter, make sure that you also check (tick) **Client for Microsoft Networks** and **File & Printer Sharing for Microsoft Networks** as shown above.

5. If configuring IPv4 addresses select **Internet Protocol Version (TCP/IPv4)**, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) with a subnet mask of 255.255.255.255, e.g. 192.168.2.20/255.255.255.255 as shown below:
6. If configuring IPv6 addresses select Internet Protocol Version (TCP/IPv6), 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:

7. Click OK on TCP/IP Properties, then click Close on Ethernet Properties to save and apply the new settings.

Note | For Windows 2012/2016/2019, it's not necessary to modify the interface metric on the advanced tab and should be left set to Automatic.

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

To configure the correct strong/weak host behavior for Windows 2012/2016/2019, the following commands must be
run on each Real Server:

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 these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```bash
netsh interface ipv4 set interface "LAN" 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
```

For these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```bash
netsh interface ipv6 set interface "LAN" 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
```

Note: The names for the NICs are case sensitive, so make sure that the name used for the interface and the name used in the commands match exactly.

- Start PowerShell or use a command window to run the appropriate netsh commands as shown in the example below:
Note | This shows an IPv6 example, use the IPv4 commands if you’re using IPv4 addresses.

Repeat steps 1 - 3 on all remaining Windows 2012/2016/2019 Real Server(s).

If preferred you can also use the following PowerShell Cmdlets:

The following example configures both IPv4 and IPv6 at the same time:

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

To configure just IPv4:

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

To configure just IPv6:

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

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 the section 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.

**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 should be configured first, 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</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>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,</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>Firewall connection tracking table size, NIC offloading, SMTP relay,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logging and Syslog Server</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>

**Important**

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

To add a Secondary node - i.e. create a highly available 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 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:
To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen.

**Note**
Clicking the **Restart Heartbeat** button on the 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](#).
18. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>3 July 2018</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>5 July 2018</td>
<td>Replaced an irrelevant note with a new note about configuring HA in the Output Manager Server Configuration Utility</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.2</td>
<td>6 December 2018</td>
<td>Added the new &quot;Company Contact Information&quot; page</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>10 December 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.1</td>
<td>8 June 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>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New screenshots for creating layer 7 VIPs</td>
<td>Changes to the appliance WebUI</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.2</td>
<td>15th October 2020</td>
<td>Name change from Nuance to Kofax</td>
<td>Kofax Acquisition of Nuance Document Imaging</td>
<td>OW</td>
</tr>
<tr>
<td>1.2.0</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>
</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.