Load Balancing Kofax ControlSuite®
v1.0.1
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 relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported
All our products can be used for load balancing Kofax ControlSuite. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td>Enterprise R320</td>
<td>Enterprise 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
<tr>
<td></td>
<td>Enterprise GCP **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: http://www.loadbalancer.org/products/hardware

** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- V7.6.4 and later

4. Kofax ControlSuite Software Versions Supported

- Kofax ControlSuite – all versions
5. 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.

6. Load Balancing Kofax ControlSuite

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”.

7. Load Balancer Deployment Methods

The load balancer can be deployed in 4 fundamental ways: Layer 4 DR mode, Layer 4 NAT mode, Layer 4 SNAT mode and Layer 7 SNAT mode. However, we will only be using Layer 4 DR mode, Layer 4 NAT mode or Layer 7 SNAT modes in this guide.

Layer 4 DR Mode

One-arm direct routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.
• 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 Servers own IP address and the VIP.

• The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as **Solving the ARP Problem**. Please refer to page 38 for more information.

• 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 in DR mode i.e. having a different RIP port than the VIP port.

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

**Layer 4 NAT Mode**

Layer 4 NAT mode is typically deployed in a two arm fashion although it can also support single arm. Inbound requests are received at the load balancer and translated changing the destination IP address before forwarding traffic on to the real server. Return traffic MUST come back through the load balancer in order for the traffic to be translated on the way back to the client. As a result, Layer 4 NAT is a less scalable technique when compared to DR because reply traffic needs to come back via the load balancer.
Servers. However, since the load balancer is acting as a full proxy it doesn't have the same raw throughput as the layer 4 methods.

The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

- The load balancer translates all requests from the external Virtual Service to the internal Real Servers.
- Normally eth0 is used for the internal network and eth1 is used for the external network although this is not mandatory. If the Real Servers require Internet access, Autonat should be enabled using the WebUI option: Cluster Configuration > Layer 4 – Advanced Configuration, the external interface should be selected.
- NAT mode can be deployed in the following ways:
  
  **2-arm (using 2 Interfaces), 2 subnets** (as shown above) - One interface on the load balancer is connected to subnet1 and the second interface and Real Servers are connected to subnet2. The VIP is brought up in subnet1. The default gateway on the Real Servers is set to be an IP address in subnet2 on the load balancer. Clients can be located in subnet1 or any remote subnet provided they can route to the VIP.
  
  **2-arm (using 1 Interface), 2 subnets** - same as above except that a single interface on the load balancer is allocated 2 IP addresses, one in each subnet.
  
  **1-arm (using 1 Interface), 1 subnet** - Here, the VIP is brought up in the same subnet as the Real Servers. For clients located in remote networks the default gateway on the Real Servers must be set to be an IP address on the load balancer. For clients located on the same subnet, 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 details on ‘One-Arm NAT Mode’ refer to page 113 of our administration manual.
  
  - If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. SMTP or RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this - please refer to page 113 of our administration manual for more details.
  
  - NAT 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 request to the chosen Real Server. As a result, Layer 7 is a slower technique than DR or NAT mode at Layer 4. 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.
This mode can be deployed in a one-arm or two-arm configuration and does not require any changes to the Real Servers. However, since the load balancer is acting as a full proxy it doesn't have the same raw throughput as the layer 4 methods.

The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

- SNAT mode is a full proxy and therefore load balanced Real Servers do not need to be changed in any way.
- Because SNAT mode is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN.
- 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 balancers 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 clients IP address can be passed through either by enabling TProxy on the load balancer, or for HTTP, using X-forwarded-For headers. Please refer to chapter 6 in the administration manual for more details.
- SNAT mode can be deployed using either a 1-arm or 2-arm configuration.
8. Appliance Configuration for Kofax Equitrac – Using DR Mode

Prerequisites
A load balanced Kofax Equitrac environment requires the following:

- Microsoft Windows Server environment
- Installation of DCE server

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

Note: The steps listed here are for a version 8.x Loadbalancer.org appliance, however the steps are similar for all versions

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
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.
9. Appliance Configuration for Microsoft Print Servers (Optional) – Using SNAT Mode

Note: The steps listed here are for a version 8.x Loadbalancer.org appliance, however the steps are similar for all versions

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

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 blue box that appears. This will apply the new changes and put the new virtual service and its associated virtual servers into use.

### 10. 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 Appendix 1 on page 38 for more information.

**Note:** 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

### 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

**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:** EQDCEHA

---

*Note:* 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

**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 TCPIIP should be disabled on all interfaces of each print server, like 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.

Note: 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
3. NetBIOS broadcast
4. Local LMHosts file
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
```

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

**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.
11. 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
- ‘Route components’ to deliver documents to virtually any destination such as fax, email, network folders, PCs, and document management systems

12. Load Balancing Kofax AutoStore

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

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.

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.
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.

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:


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

14. Configuring Kofax AutoStore for Load Balancing

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 the ‘Other Vendors’ section on page 18
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 section of the appendix on page 38 for more information.

For a detailed explanation of DR mode and the nature of the ARP problem, please refer to the section that covers layer 4 DR mode on page 6.

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

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 the 'Other Vendors' section on page 18
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]

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]
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

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


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 the ‘Other Vendors’ section on page 18
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**
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

17. Testing & Verification

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

Using 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 the each cluster as a whole. The example below shows that all AutoStore servers are healthy and available to accept connections.
18. 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

19. 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>

20. Output Manager Deployment Concept

VIPs = Virtual IP Addresses

© Copyright Loadbalancer.org - www.loadbalancer.org - sales@loadbalancer.org
21. 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 section of the appendix on page 38 for more information.

For a detailed explanation of DR mode and the nature of the ARP problem, please refer to the section that covers layer 4 DR mode on page 6.

22. 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
6. Leave the Forwarding Method set to Direct Routing
7. Click Update to create the virtual service
**Layer 4 - Add a new 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>Ports</td>
<td>445</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
</tbody>
</table>

8. Click **Modify** next to the newly created VIP
9. 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>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>Check Type</td>
</tr>
<tr>
<td></td>
<td>Connect to port</td>
</tr>
<tr>
<td></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](image)

**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

![Layer 4 - Add a new Virtual Service](image)
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](image)

### 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
23. 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 **Port** 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
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

---

**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
Finalizing the Configuration
To apply the new settings, HAProxy must be restarted as follows:

1. Using the WebUI, navigate to: Maintenance > Restart Services and click Restart HAProxy

24. Testing & Verification

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 the appendix section on page 45 for more information.

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.
25. 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.

26. Further Documentation

27. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Kofax Equitrac environments.
1 - 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 2012/2016, for other versions of Windows please refer to chapter 6 in the administration manual.

Step 1: 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

![Add Hardware](image)

6. Click Next to start the installation, when complete click Finish

Step 2: 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. Un-check 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 to solve the ARP Problem, the following options **must** also be checked (ticked):

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

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.

8. Now repeat the above process on the other Windows 2012/2016 Real Servers.
Step 3: Configure the strong/weak host behavior

Windows Server 2000 and Windows Server 2003 use the weak host model for sending and receiving for all IPv4 interfaces and the strong host model for sending and receiving for all IPv6 interfaces. You cannot configure this behavior. The Next Generation TCP/IP stack in Windows 2008 and later supports strong host sends and receives for both IPv4 and IPv6 by default. To ensure that Windows 2012/2016 is running in the correct mode to be able to respond to the VIP, the following commands must be run on each Real Server:

For IPv4 addresses:

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

For IPv6 addresses:

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

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:

For IPv4 addresses:

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:

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

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:
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.

1. 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.

2. Now repeat these 4 commands on the other Windows 2012/2016 Real Servers

   Note: Solving the ARP problem for other version of Windows is similar. For full details, please refer to the [administration manual](#).
2 – Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

Note: A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
- Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
- SNMP settings
- Graphing settings
- Firewall Script & Firewall Lockdown Script settings
Software updates

Version 7:

Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8:

To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration
• Specify the IP address and the loadbalancer users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above

• Click Add new node

• The pairing process now commences as shown below:

![Create a Clustered Pair](image)

• Once complete, the following will be displayed:

![High Availability Configuration - Master](image)

• 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 master appliance will also automatically restart heartbeat on the slave appliance.

Note: Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
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 section Configuring Name Resolution on page 27.

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
# 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>
</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.

United Kingdom
Loadbalancer.org Ltd.
Compass House, North Harbour Business Park, Portsmouth, PO6 4PS
UK:+44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

Canada
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver, BC, V6B 2Z4, Canada
TEL:+1 866 998 0508
sales@loadbalancer.org
support@loadbalancer.org

United States
Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

Germany
Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org

© Copyright Loadbalancer.org • www.loadbalancer.org