Load Balancing Kofax AutoStore

Version 1.2.0
Table of Contents

1. About this Guide ................................................................. 3
2. Loadbalancer.org Appliances Supported ................................ 3
3. Loadbalancer.org Software Versions Supported ...................... 3
4. Kofax AutoStore Software Versions Supported ....................... 3
5. Kofax AutoStore ................................................................. 3
6. Load Balancing Kofax AutoStore .......................................... 3
   Load Balancing & HA Requirements ..................................... 3
   Persistence (aka Server Affinity) ........................................ 4
   Virtual Service (VIP) Requirements .................................... 4
   Port Requirements .......................................................... 4
     Xerox EIP Connect .......................................................... 4
     Konica Minolta ............................................................. 4
     Ricoh ESA ................................................................. 4
     Ricoh SOP ................................................................. 5
     Other Vendors ............................................................ 5
7. Deployment Concept .......................................................... 5
8. Load Balancer Deployment Methods ...................................... 5
   Layer 4 DR Mode ............................................................. 6
   Layer 4 NAT Mode ............................................................ 6
   Our Recommendation ....................................................... 8
9. Configuring Kofax AutoStore for Load Balancing ..................... 8
   Device Registration Service Configuration ............................ 8
   Layer 4 DR Mode – Solving the ARP Problem ......................... 9
10. Loadbalancer.org Appliance – the Basics ............................... 9
    Virtual Appliance .......................................................... 9
    Initial Network Configuration ............................................ 10
    Accessing the WebUI ....................................................... 10
      Main Menu Options ....................................................... 11
      HA Clustered Pair Configuration ..................................... 12
11. Appliance Configuration for Kofax AutoStore – Using Layer 4 DR Mode ................................................................. 12
    Configuring the Virtual Service (VIP) ................................ 12
    Defining the Real Servers (RIPs) ....................................... 13
12. Appliance Configuration for Kofax AutoStore – Using Layer 4 NAT Mode ................................................................. 14
    Configuring the Virtual Service (VIP) ................................ 14
    Defining the Real Servers (RIPs) ....................................... 15
13. Testing & Verification .......................................................... 16
    Testing Using a Multi-function Device ................................. 16
      Using System Overview ................................................... 16
14. Technical Support ............................................................. 16
15. Further Documentation ...................................................... 16
16. Conclusion ................................................................. 16
17. Appendix ........................................................................ 17
    Solving the ARP Problem .................................................. 17
      Windows Server 2012, 2016 & 2019 ................................ 17
      Configuring HA - Adding a Secondary Appliance ................. 21
18. Document Revision History ................................................. 25
1. About this Guide

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

- V8.3.8 and later

4. Kofax AutoStore Software Versions Supported

- Kofax AutoStore – version 7.0

5. 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

6. 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>
### Other Vendors

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

https://knowledge.kofax.com/MFD_Productivity/AutoStore/Configuration/AutoStore_7_Default_ports_for_capture_process_and_route_components

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

### 7. Deployment Concept

VIPs = Virtual IP Addresses

**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 either Layer 4 DR mode or Layer 4 NAT mode.

For Kofax AutoStore, layer 4 DR mode is recommended unless a two arm configuration is needed. 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 AutoStore – Using Layer 4 DR Mode, and for configuring using layer 4 NAT mode refer to Appliance Configuration for Kofax AutoStore – Using Layer 4 NAT 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 4 NAT Mode

Layer 4 NAT mode is a high performance solution, although not as fast as layer 4 DR mode. This is because real server responses must flow back to the client via the load balancer rather than directly as with DR mode.
The load balancer translates all requests from the 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:

**Two-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.

**Two-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.

**One-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 information please refer to *One-Arm (Single Subnet) NAT Mode*.

- If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. 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.
- Port translation is possible with Layer 4 NAT mode, e.g. VIP:80 \(\rightarrow\) RIP:8080 is supported.
- NAT mode is transparent, i.e. the Real Server will see the source IP address of the client.

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

The following table shows an example NAT mode setup:

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

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

Packet rewriting works as follows:

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

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

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

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

3) Replies return to the load balancer as:

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

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

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

**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 required to use a 2-arm configuration, then layer 4 NAT mode is recommended.

**9. 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 `Other Vendors`

Note: If any configuration changes are made to the AutoStore real servers they will need to be unregistered and then re-registered in the Device Registration Service for the configurations to be accepted.

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.
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.

Please refer to The Virtual Appliance - Hypervisor Deployment and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.

**Initial Network Configuration**

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway, DNS 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. Appliance authentication is based on Apache .htaccess files. User admin tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.

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.

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
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 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 Other Vendors

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. 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**

<table>
<thead>
<tr>
<th>Label</th>
<th>AutoStore-KonicaMinolta</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.85.10</td>
</tr>
<tr>
<td>Ports</td>
<td>3348,13351,13353,13391</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>Timeout</td>
<td>300 seconds</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. 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.

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service.

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

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

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

5. Set the Forwarding Method to NAT.

6. Click Update to create the virtual service.

7. Click Modify next to the newly created VIP.

8. Set Balance Mode to Weighted Round Robin.

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

10. Click Update.
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.
13. 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.

### System Overview

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th>IP</th>
<th>Ports</th>
<th>Conn</th>
<th>Protocol</th>
<th>Method</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoStore-Xerox</td>
<td>192.168.85.10</td>
<td>3241</td>
<td>0</td>
<td>TCP</td>
<td>Layer 4</td>
<td>DR</td>
</tr>
<tr>
<td>AutoStore1</td>
<td>192.168.85.20</td>
<td>3241</td>
<td>100</td>
<td>TCP</td>
<td>Drain</td>
<td>Halt</td>
</tr>
<tr>
<td>AutoStore2</td>
<td>192.168.85.21</td>
<td>3241</td>
<td>100</td>
<td>TCP</td>
<td>Drain</td>
<td>Halt</td>
</tr>
<tr>
<td>AutoStore3</td>
<td>192.168.85.22</td>
<td>3241</td>
<td>100</td>
<td>TCP</td>
<td>Drain</td>
<td>Halt</td>
</tr>
</tbody>
</table>

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 AutoStore environments.
17. Appendix

Solving the ARP Problem
Windows Server 2012, 2016 & 2019

The basic concept is the same as for Windows 2000/2003. However, additional steps are required to set the strong/weak host behavior. This is used to either block or allow interfaces receiving packets destined for a different interface on the same server. As with Windows 2000/2003/2008, if the Real Server is included in multiple VIPs, you can add additional IP addresses to the Loopback Adapter that correspond to each VIP.

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

When configuring the Loopback Adapter to solve the ARP Problem 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:

```
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:

```
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 "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:

```
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).

For Windows 2012/2016/2019 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
```

**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.
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.

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 Configuration</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced Configuration</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server</td>
</tr>
<tr>
<td>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>

To add a Secondary node - i.e. create a highly available clustered pair:

1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI, 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:

7. To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen.
Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

For more details on configuring HA with 2 appliances, please refer to **Appliance Clustering for HA**.
## 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>21 June 2018</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>26 June 2018</td>
<td>Made the guide more generic by adding additional vendor options</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed the title from 'AutoStore With Xerox EIP Connect'</td>
<td></td>
<td></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>1 August 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AW, AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed layer 7 SNAT mode deployment method to layer 4 NAT mode</td>
<td>Required updates</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated a Kofax hyperlink to use the new Kofax location</td>
<td></td>
<td></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></td>
</tr>
<tr>
<td>1.1.2</td>
<td>15 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.