# Table of Contents

1. About this Guide ................................................................. 4
2. Loadbalancer.org Appliances Supported ................................. 4
3. Loadbalancer.org Software Versions Supported ....................... 4
4. Konica Minolta Dispatcher Phoenix Software Versions Supported . 4
5. Konica Minolta Dispatcher Phoenix ..................................... 4
6. Load Balancing Konica Minolta Dispatcher Phoenix ................. 4
7. Load Balancer Deployment Methods ..................................... 5
   - Layer 4 DR Mode ............................................................ 5
   - Layer 7 SNAT Mode ....................................................... 6
8. Dispatcher Phoenix Deployment Concept ............................... 6
9. Load Balancing Konica Minolta Dispatcher Phoenix ..................... 7
   - Load Balancing & HA Requirements .................................. 7
   - Persistence (aka Server Affinity) ..................................... 7
   - Virtual Service (VIP) Requirements ................................ 7
   - Port Requirements .......................................................... 8
     - KMBS BEST Server ..................................................... 8
     - KMBS LPR Service ..................................................... 8
     - KMBS SMTP Service ................................................... 8
     - KMBS SEC Workflow Worker Process ............................ 8
10. Loadbalancer.org Appliance – the Basics ............................... 8
    - Virtual Appliance .......................................................... 8
    - Initial Network Configuration ........................................ 9
    - Accessing the WebUI ..................................................... 9
    - Main Menu Options ....................................................... 10
    - HA Clustered Pair Configuration ................................... 11
11. Load Balancing Konica Minolta Dispatcher Phoenix – Using DR Mode . 11
    - Part 1 – Prepare the Konica Minolta Servers for Load Balancing . 11
      - Step 1 – Prerequisites ................................................ 11
      - Step 2 – Solve the ARP Problem on Each server ............... 11
      - Step 3 – Configure Registry Entries ............................. 11
      - Step 4 – Configure Name Resolution ............................. 12
      - Step 5 – Reboot Each Print Server ............................... 12
    - Part 2 – Configure Load Balancing for Microsoft Print Server .... 12
      - Configure the virtual service (VIP) .............................. 12
      - Define the Real Servers (RIPs) .................................... 13
    - Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix .... 13
      - Configure the virtual service (VIP) .............................. 13
      - Define the Real Servers (RIPs) .................................... 14
12. Load Balancing Konica Minolta Dispatcher Phoenix – Using SNAT Mode ........... 15
    - Part 1 – Prepare the Konica Minolta Servers for Load Balancing . 15
      - Step 1 – Prerequisites ................................................ 15
      - Step 2 – Configure Registry Entries ............................. 15
      - Step 3 – Configure Name Resolution ............................. 15
      - Step 4 – Reboot Each Print Server ............................... 16
    - Part 2 – Configure Load Balancing for Microsoft Print Server .... 16
      - Configure the virtual service (VIP) .............................. 16
      - Define the Real Servers (RIPs) .................................... 17
    - Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix .... 17
      - Configure the virtual service (VIP) .............................. 17
1. About this Guide

This guide details the steps required to configure a load balanced Konica Minolta Dispatcher Phoenix environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Konica Minolta Dispatcher Phoenix 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 with Konica Minolta Dispatcher Phoenix. 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. Konica Minolta Dispatcher Phoenix Software Versions Supported

- Konica Minolta Dispatcher Phoenix – all versions

5. Konica Minolta Dispatcher Phoenix

Konica Minolta’s Dispatcher Phoenix is a powerful application that can help any business save time by automating document image processing, printing, and routing tasks via customizable workflows. With a large variety of processing features, virtually everything is possible – from cleaning up images, applying watermarks and annotations, and renaming files to routing documents to folders, FTP servers, MFPs, or e-mail recipients – and it’s all fully automatic! Unique LiveFlo technology provides a real-time view of documents as they are being processed – a great way to identify bottlenecks and making sure files will reach their correct destinations. Dispatcher Phoenix provides busy offices with the convenience and flexibility they need.

The application is highly scalable up to the largest enterprise environments. Dispatcher Phoenix includes a web user interface for access to important enterprise tools – such as apps for setting up server clusters for redundancy/load balancing, failover, offloading, sharing workflows with specific users, and more. Administrators can manage their workflows (run, stop, pause) from the web as well as edit user variables and view important analytics about work being done, including the number of documents being scanned, files collected, and users scanning.

6. Load Balancing Konica Minolta Dispatcher Phoenix

For Konica Minolta Dispatcher Phoenix, the preferred load balancing method is Layer 4 DR Mode (Direct Routing, aka DSR / Direct Server Return). 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 Solving the ARP Problem.

Where it’s not feasible to use layer 4 DR mode, layer 7 SNAT mode should be used. Whist this mode does not have the raw throughput of layer 4 methods, it still enables high performance load balancing and requires no changes to
7. Load Balancer Deployment Methods

As mentioned above, Layer 4 DR mode and Layer 7 SNAT mode can be used. Both methods are described below.

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 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.

Layer 7 SNAT mode is a full proxy and therefore load balanced Real Servers do not need to be changed in any way.

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.

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

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

8. Dispatcher Phoenix Deployment Concept
VIPS = Virtual IP Addresses

9. Load Balancing Konica Minolta Dispatcher Phoenix

Note It’s highly recommended that you have a working Konica Minolta Dispatcher Phoenix environment first before implementing the load balancer.

Load Balancing & HA Requirements

In order to be successfully load balanced, a Konica Minolta Dispatcher Phoenix deployment must include 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 Dispatcher Phoenix deployment will already feature all of these components.

Persistence (aka Server Affinity)

Source IP address persistence is used for Dispatcher Phoenix servers. This ensures that a particular client will connect to the same Dispatcher Phoenix server for the duration of the session.

Virtual Service (VIP) Requirements

To provide load balancing and HA for Dispatcher Phoenix, 2 VIPs are used. The first VIP is for the underlying Microsoft print services and the second VIP is for the particular Konica Minolta service being load balanced.
Port Requirements
The following tables show the ports that are load balanced for the various Konica Minolta services:

### KMBS BEST Server

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>50808</td>
<td>HTTP</td>
<td>KMBS BEST Server</td>
</tr>
<tr>
<td>50809</td>
<td>HTTPS</td>
<td>Secure BEST Server</td>
</tr>
</tbody>
</table>

### KMBS LPR Service

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>515</td>
<td>TCP</td>
<td>LPR Service (LPD)</td>
</tr>
</tbody>
</table>

### KMBS SMTP Service

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TCP</td>
<td>Default, but configurable within SMTP Manager</td>
</tr>
</tbody>
</table>

### KMBS SEC Workflow Worker Process

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>53</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>465</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
<tr>
<td>587</td>
<td>TCP</td>
<td>Output Port</td>
</tr>
</tbody>
</table>

### 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.
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. 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.

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>

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

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

**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. Load Balancing Konica Minolta Dispatcher Phoenix – Using DR Mode

Part 1 – Prepare the Konica Minolta Servers for Load Balancing

Step 1 – Prerequisites

For a load balanced Konica Minolta Dispatcher Phoenix environment, each print server must comply with the following requirements:

1. Be a member of a Microsoft Windows Domain.
2. Have the Print and Document Service role / Print Server service installed.
3. Have all required printers installed and shared – the share names and permissions must be the same across all servers.
4. Have Konica Minolta Dispatcher Phoenix installed.

Step 2 – Solve the ARP Problem on Each server

When using layer 4 DR mode, the "ARP problem" must be solved on each print 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.

Step 3 – Configure Registry Entries

For the load balanced print servers, to enable them to be accessed via a shared name (Dispatcher 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: Dispatcher
```
Note

In the example presented here, Dispatcher 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.

Step 4 – Configure Name Resolution

For printer load balancing to work, DNS name resolution should be configured. A DNS Host (A) record for the printer share name (Dispatcher in this example) that points at the Phoenix Dispatcher VIP (192.168.81.10 in this example) is required.

In addition, NetBIOS over TCP/IP should be disabled on all interfaces on each print server as shown below:

![Advanced TCP/IP Settings](image)

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

Step 5 – Reboot Each Print Server

To apply all settings, reboot each print server.

Part 2 – Configure Load Balancing for Microsoft Print Server

Configure 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. PrintServers.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.81.10.

4. Set the Ports to 445.

5. Leave Protocol set to TCP.


7. Click Update.

Define 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. PS1.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.81.184.

4. Click Update.

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

Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix

Configure 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. Dispatcher.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.81.10.

4. Set the Ports field according to the load balanced service – please refer to Port Requirements.

Note
If you are load balancing "KMBS SEC Workflow Worker Process", exclude port 445 from the list of ports since this port is load balanced by the Microsoft Print Server VIP configured previously.

5. Leave Protocol set to TCP.


7. Click Update.

8. Click Modify next to the newly created VIP.

9. Scroll down to the Health Checks section and set the Check Port to 445.

10. Click Update.

Define 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. Phoenix1.

3. Set the *Real Server IP Address* field to the required IP address, e.g. 192.168.81.184.

4. Click Update.

5. Repeat these steps to add additional Dispatcher Phoenix servers as required.

12. Load Balancing Konica Minolta Dispatcher Phoenix – Using SNAT Mode

**Part 1 – Prepare the Konica Minolta Servers for Load Balancing**

**Step 1 – Prerequisites**

For a load balanced Konica Minolta Dispatcher Phoenix environment, each print server must comply with the following requirements:

1. Be a member of a Microsoft Windows Domain.

2. Have the *Print and Document Service* role / *Print Server* service installed.

3. Have all required printers installed and shared – the share names and permissions must be the same across all servers.

4. Have Konica Minolta Dispatcher Phoenix installed.

**Step 2 – Configure Registry Entries**

For the load balanced print servers, to enable them to be accessed via a shared name (*Dispatcher* 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**: Dispatcher

**Note**

In the example presented here, *Dispatcher* 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.

**Step 3 – Configure Name Resolution**

For printer load balancing to work, DNS name resolution should be configured. A DNS Host (A) record for the printer share name (*Dispatcher* in this example) that points at the Phoenix Dispatcher VIP (192.168.81.10 in this example) is required.
In addition, NetBIOS over TCP/IP should be disabled on all interfaces on each print server as shown below:

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

Step 4 – Reboot Each Print Server
To apply all settings, reboot each print server.

Part 2 – Configure Load Balancing for Microsoft Print Server
Configure 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. PrintServers.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.81.10.

4. Set the Ports to 445.

5. Set the Layer 7 Protocol to TCP Mode.

6. Click Update.

Define 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.

- **Label**: PS1
- **Real Server IP Address**: 192.168.81.184
- **Real Server Port**: Blank
- **Re-Encrypt to Backend**: Blank
- **Weight**: 100

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. 192.168.81.184.

4. Leave the Real Server Port field blank.

5. Click Update.

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

Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix

Configure 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. Dispatcher.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.81.10.

4. Set the Ports field according to the load balanced service – please refer to Port Requirements.

   Note: If you are load balancing "KMBS SEC Workflow Worker Process", exclude port 445 from the list of ports since this port is load balanced by the Microsoft Print Server VIP configured previously.

5. Set the Layer 7 Protocol to TCP Mode.

6. Click Update.

7. Click Modify next to the newly created VIP.

8. Scroll down to the Health Checks section and set the Check Port to 445.

9. Click Update.

Define 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. Phoenix1.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.81.184.
4. Leave the *Real Server Port* field blank.
5. Click **Update**.
6. Repeat these steps to add additional print servers as required.

**Finalize Settings – Reload HAProxy**
To apply settings and activate the new VIPs, click the **Reload** button in the blue box at the top of the screen.

**13. Testing & Verification**

Note For additional general guidance please also refer to *Testing Load Balanced Services.*

**Testing the Load Balanced Servers**
The load balanced servers can be tested either by browsing to the virtual service IP address or to the printer share name. For example:

Using the Virtual IP address (VIP):

\192.168.81.10

or

Using the printer share name:

\Dispatcher

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

**Using System Overview**
The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Dispatcher Phoenix servers) and shows the state/health of each server as well as the state of each cluster as a whole.

The example below shows that all Real Servers are healthy and available to accept connections.
Note: This example shows layer 4 VIPs. A layer 7 configuration will look very similar.

If a particular server fails its health check, that server will be displayed red rather than green.

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 Konica Minolta Dispatcher Phoenix environments.
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:
Note: Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred.

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:
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:

```plaintext
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:

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

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:

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

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4

To configure just IPv6:

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.

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.

Note

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>WebUI Main Menu Option</td>
<td>Sub Menu Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>

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 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:

**High Availability Configuration - primary**

7. 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**.
## 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 October 2020</td>
<td>Initial version</td>
<td></td>
<td>NH / RJC</td>
</tr>
<tr>
<td>1.0.1</td>
<td>25 March 2021</td>
<td>Added section &quot;Loadbalancer.org Appliance – the Basics&quot;</td>
<td>Not included in the initial version</td>
<td>RJC</td>
</tr>
<tr>
<td>1.1.0</td>
<td>1 October 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.