1. About this Guide

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

Note

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

4. Pharos Blueprint Software Versions Supported

- Pharos Blueprint Enterprise v5.3 & Later

5. Pharos Blueprint

Pharos Blueprint gives you critical insights into your print environment and workflows, empowering you to successfully manage print and its related costs. Blueprint is a single system with the flexibility to work with a mix and match of equipment manufacturers and device models. Blueprint makes it easy to manage your entire print environment. Blueprint delivers secure printing and significant cost savings and waste reduction. It provides the information you need to optimize your equipment fleet, improve employee printing habits, and take meaningful action today and throughout the future.

6. Load Balancing Pharos Blueprint

Note

It’s highly recommended that you have a working Pharos Blueprint environment first before implementing the load balancer.

Load Balancing & HA Requirements

2 or more Collector servers are configured to create a load balanced pool. Clients then connect to this pool via Virtual Services (VIPs).
Port Requirements
The following tables show the ports that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>808</td>
<td>TCP</td>
<td>Server to Server Communications (Analyst to Collector, Collector to Collector) Administrator to Server Communications  808 is used by the Administrator to the TaskMaster. It is encrypted. Anything the Administrator tool wants is pulled by TaskMaster service and given to Administrator over 808</td>
</tr>
<tr>
<td>8080</td>
<td>TCP</td>
<td>Server to Server Communications (Analyst to Collector, Collector to Collector) Administrator to Server Communications 8080 is how Collectors upload their transaction info and provide status update/health check info to the Analyst, and how the Analyst updates its own health check Client to Server Communication (View waiting print jobs)</td>
</tr>
<tr>
<td>9001</td>
<td>TCP</td>
<td>Used for inter-server communications between the Pharos Systems Secure Release Service and the MobilePrint Worker service</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>Microsoft Print/SMB Services</td>
</tr>
</tbody>
</table>

Pharos Blueprint Deployment Concept

VIP = Virtual IP Addresses
Virtual Service (VIP) Requirements

To provide load balancing and HA for Pharos Blueprint, 4 VIPs are used. Three VIPs for the Pharos Blueprint services, and a fourth for the underlying Microsoft print services.

Supported Load Balancer Deployment Methods

For Pharos Blueprint, both layer 4 DR mode and layer 7 SNAT mode can be used, although for maximum throughput the preferred 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 Collector 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. Whilst this mode does not have the raw throughput of layer 4 methods, it still enables high performance load balancing and requires no changes to the Collector Servers.

Each Mode is 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.

**Note** Kemp, Brocade, Barracuda & A10 Networks call this *Direct Server Return* and F5 call it *N-Path*.

- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Server's own IP address and the VIP.
- The Real Servers should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as *Solving the ARP Problem*. For more information please refer to DR Mode Considerations.
- On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP.
The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work.

The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet.

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

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

Layer 7 SNAT Mode
Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer and HAPerxy generates a new corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.

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

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

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

Requires no additional configuration changes to the load balanced Real Servers.

Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.
• You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

7. Loadbalancer.org Appliance – the Basics

Virtual Appliance
A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.

Note | The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance’s WebUI.

Note | Please refer to 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.

Note | 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.

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

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

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

2. Log in to the WebUI:

Username: loadbalancer
Password: <configured-during-network-setup-wizard>

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

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

Note | The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.
3. You'll be asked if you want to run the Setup Wizard. If you click **Accept** the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simply click **Dismiss**.

**Main Menu Options**

- **System Overview** - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
- **Local Configuration** - Configure local host settings such as IP address, DNS, system time etc.
- **Cluster Configuration** - Configure load balanced services such as VIPs & RIPs
- **Maintenance** - Perform maintenance tasks such as service restarts and taking backups
- **View Configuration** - Display the saved appliance configuration settings
- **Reports** - View various appliance reports & graphs
- **Logs** - View various appliance logs
- **Support** - Create a support download, contact the support team & access useful links
- **Live Chat** - Start a live chat session with one of our Support Engineers

**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, and adding a secondary unit is covered in Configuring HA - Adding a Secondary Appliance.

### 8. Load Balancing Pharos Blueprint – Using Layer 4 DR Mode

**STEP 1 – Prepare the Pharos Blueprint Servers for Load Balancing**

**A) Prerequisites**

For a load balanced Pharos Blueprint environment, each Collector Server must comply with the following requirements:

- Be a member of a Microsoft Windows Domain
- Have the Print and Document Service role / Print Server service installed
- Have all required printers installed and shared – the share names and permissions must be the same across all servers
- Have Pharos Blueprint installed

**B) Solve the ARP Problem on Each server**

When using layer 4 DR mode, the "ARP problem" must be solved on each Collector 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](#).

**C) Enable Print Server Load Balancing**

To enable the load balanced Collector Servers to be accessed via a shared name (blueprintservice is the example used in this guide), the following steps must be completed:

**Windows 2019**

Host entries must be added to the local hosts file on each Collector Server. For example, if you have 2 Collector Servers: 192.168.81.11 and 192.168.81.12, add the following entries to the hosts files:
On the 192.168.81.11 server:

192.168.81.11 blueprintservice
192.168.81.11 blueprintservice.yourdomain.com

On the 192.168.81.12 server:

192.168.81.12 blueprintservice
192.168.81.12 blueprintservice.yourdomain.com

where **blueprintservice** is the DNS name clients use to access the load balanced Collector Servers.

### Windows 2012 & 2016

Configure the following Registry entries:

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: blueprintservice

**Note**

In the example presented here, **blueprintservice** is the name that will be used to access the load balanced Collector Servers via the VIPs created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address used for the VIPs.

**D) Configure Name Resolution**

To enable clients to connect via the load balancer, DNS name resolution must be configured. Create a DNS Host (A) record for the printer share name (**blueprintservice** in this example) that points at the IP address used for the VIPs (**192.168.81.10** in this example).

In addition, NetBIOS over TCP/IP should be disabled on all interfaces on each Collector Server as shown below:
E) Reboot Each Server
To apply all settings, reboot each Collector Server.

STEP 2 – Configure the VIPs & RIPv

VIP1 – Port 808
Define the VIP

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

2. Define the Label (i.e. the name) for the virtual service as required, e.g. PharosBP-808.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.81.10.
4. Set **Ports** to **808**.
5. Leave **Protocol** set to **TCP**.
6. Leave **Forwarding Method** set to **Direct Routing**.
7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Scroll down to the **Persistence** section and uncheck the **Enable** checkbox.
10. Click **Update**.

**Define the Real Servers (RIPs)**

1. Using the WebUI, navigate to **Cluster Configuration > Layer 4 – Real Servers** and click on **Add a new Real Server** next to the newly created VIP.

   ![Real Server Table](image)

   - **Label**: Collector1
   - **Real Server IP Address**: 192.168.81.11
   - **Weight**: 100
   - **Minimum Connections**: 0
   - **Maximum Connections**: 0

2. Define the **Label** (i.e. the name) for the Real Server as required, e.g. **Collector1**.
3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.81.11**.
4. Click **Update**.
5. Repeat these steps to add additional Collector Servers as required.

**VIP2 – Port 8080**

- Click **Modify** next to the **PharosBP-808** VIP just created, then click **Duplicate Service**.
- Change the VIP **label** to an appropriate name, e.g. **PharosBP-8080**.
- Change the VIP **Ports** to **8080**.
- Leave all other settings the same.
- Click **Update** to save the new VIP.

**VIP3 – Port 9001**

- Again, duplicate the **PharosBP-808** VIP.
- Change the VIP **label** to an appropriate name, e.g. **PharosBP-9001**.
- Change the VIP **Ports** to **9001**.
- Leave all other settings the same.

STEP 1 – Prepare the Pharos Blueprint Servers for Load Balancing

A) Prerequisites
For a load balanced Pharos Blueprint environment, each Collector Server must comply with the following requirements:

- Be a member of a Microsoft Windows Domain
- Have the Print and Document Service role / Print Server service installed
- Have all required printers installed and shared – the share names and permissions must be the same across all servers
- Have Pharos Blueprint installed

B) Enable Print Server Load Balancing
To enable the load balanced Collector Servers to be accessed via a shared name (blueprintservice is the example used in this guide), the following steps must be completed:

*Windows 2019*

Host entries must be added to the local hosts file on each Collector Server. For example, if you have 2 Collector Servers: 192.168.81.11 and 192.168.81.12, add the following entries to the hosts files:

On the 192.168.81.11 server:

```
192.168.81.11 blueprintservice
192.168.81.11 blueprintservice.yourdomain.com
```

On the 192.168.81.12 server:

```
192.168.81.12 blueprintservice
192.168.81.12 blueprintservice.yourdomain.com
```

where blueprintservice is the DNS name clients use to access the load balanced Collector Servers.

*Windows 2012 & 2016*
Configure the following Registry entries:

- **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:** blueprintservice

---

**Note**

In the example presented here, **blueprintservice** is the name that will be used to access the load balanced Collector Servers via the VIPs created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address used for the VIPs.

---

**C) Configure Name Resolution**

To enable clients to connect via the load balancer, DNS name resolution must be configured. Create a DNS Host (A) record for the printer share name (**blueprintservice** in this example) that points at the IP address used for the VIPs (**192.168.81.10** in this example).

In addition, NetBIOS over TCP/IP should be disabled on all interfaces on each Collector Server as shown below:
D) Reboot Each Server
To apply all settings, reboot each Collector Server.

STEP 2 – Configure the VIPs & RIPs
VIP1 – Port 808
Define the VIP

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

2. Define the Label (i.e. the name) for the virtual service as required, e.g. PharosBP-808.

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

4. Set Ports to 808.

5. Change Layer 7 Protocol to TCP Mode.

6. Click Update.

7. Now click Modify next to the newly created VIP.

8. Scroll down to the Persistence section and change Persistence Mode to None.

9. Click Update.

Define the Real Servers (RIPs)

1. Using the WebUI, 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* (i.e. the name) for the Real Server as required, e.g. *Collector1*.

3. Set the *Real Server IP Address* field to the required IP address, e.g. *192.168.81.11*.

4. Leave *Real Server Port* blank.

5. Click *Update*.

6. Repeat these steps to add additional Collector Servers as required.

**VIP2 – Port 8080**

- Click *Modify* next to the *PharosBP-808* VIP just created, then click *Duplicate Service*.

- Change the VIP *label* to an appropriate name, e.g. *PharosBP-8080*.

- Change the VIP *Ports* to 8080.

- Leave all other settings the same.

- Click *Update* to save the new VIP.

**VIP3 – Port 9001**

- Again, duplicate the *PharosBP-808* VIP.

- Change the VIP *label* to an appropriate name, e.g. *PharosBP-9001*.

- Change the VIP *Ports* to 9001.

- Leave all other settings the same.

- Click *Update* to save the new VIP.

**VIP4 – Port 445**

- Again, duplicate the *PharosBP-808* VIP.

- Change the VIP *label* to an appropriate name, e.g. *PharosBP-445*.

- Change the VIP *Ports* to 445.

- Leave all other settings the same.

- Click *Update* to save the new VIP.

**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.
10. 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 chosen DNS name, in this guide blueprintservice.

e.g.

\blueprintservice
\blueprintservice.yourdomain.com

The shared printers that have been configured on the Collector Servers should be visible. Open/connect to the shared printers.

Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Pharos Blueprint 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.
Note This example shows layer 7 VIPs. A layer 4 configuration will look very similar.

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

11. 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.

12. Further Documentation


13. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Pharos Blueprint environments.
14. Appendix

Solving the ARP Problem

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

Windows Server 2012 & Later

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

Step 1 of 3: Install the Microsoft Loopback Adapter

1. Click Start, then run hdwwiz to start the Hardware Installation Wizard.
2. When the Wizard has started, click Next.
3. Select Install the hardware that I manually select from a list (Advanced), click Next.
4. Select Network adapters, click Next.
5. Select Microsoft & Microsoft KM-Test Loopback Adapter, click Next.

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

Step 2 of 3: Configure the Loopback Adapter

1. Open Control Panel and click Network and Sharing Center.
2. Click Change adapter settings.
3. Right-click the new Loopback Adapter and select Properties.
4. Uncheck all items except Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6) as shown below:

![Loopback Properties](image)

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

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

5. If configuring IPv4 addresses select Internet Protocol Version (TCP/IPv4), click Properties and configure the IP address to be the same as the Virtual Service (VIP) with a subnet mask of 255.255.255.255, e.g. 192.168.2.20/255.255.255.255 as shown below:
6. If configuring IPv6 addresses select Internet Protocol Version (TCP/IPv6), click Properties and configure the IP address to be the same as the Virtual Service (VIP) and set the Subnet Prefix Length to be the same as your network setting, e.g. 2001:470:1f09:e72::15/64 as shown below:

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

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

Step 3 of 3: Configure the strong/weak host behavior
To configure the correct strong/weak host behavior for Windows 2012/2016/2019, the following commands must be run on each Real Server:

For IPv4 addresses:

```
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).

If preferred you can also use the following PowerShell Cmdlets:

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

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

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:

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**.
## 15. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>3 March 2021</td>
<td>Initial version</td>
<td></td>
<td>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.