Load Balancing eCopy ShareScan

Version 1.1.0
Table of Contents

1. About this Guide ................................................................. 4
2. Loadbalancer.org Appliances Supported .................................... 4
3. Loadbalancer.org Software Versions Supported ............................ 4
4. eCopy ShareScan Software Versions Supported .......................... 4
5. eCopy ShareScan ............................................................... 4
6. Load Balancing eCopy ShareScan ............................................ 4
   The Basics .............................................................................. 4
   Ports & Protocols ..................................................................... 4
   eCopy ShareScan Server Health-checks ....................................... 5
   SSL Termination & Certificates ................................................ 5
   Persistence (aka Server Affinity) ............................................... 5
   Load Balancer Deployment ...................................................... 5
   Load Balancer Deployment Modes ........................................... 6
   Layer 4 DR Mode .................................................................... 6
   Layer 4 NAT Mode .................................................................. 7
   Loadbalancer.org Recommended Mode ....................................... 8
7. Loadbalancer.org Appliance – the Basics .................................... 8
   Virtual Appliance ..................................................................... 9
   Initial Network Configuration .................................................. 9
   Accessing the WebUI ............................................................. 9
   Main Menu Options ................................................................ 10
   HA Clustered Pair Configuration ............................................. 11
8. Appliance & eCopy ShareScan Server Configuration – Using Layer 4 DR Mode ........................................ 11
   Overview .............................................................................. 11
   Load Balancer Configuration .................................................. 11
   Configure the Network Interface ............................................. 11
   Configure the Virtual Service (VIP) ......................................... 11
   Configure the Real Servers (RIPs) ............................................ 12
   eCopy ShareScan Server Configuration .................................... 13
   Solve the ‘ARP Problem’ ....................................................... 13
   DR Mode – Key Points ......................................................... 13
   Configure ShareScan server registry settings ............................. 14
9. Appliance & eCopy ShareScan Server Configuration – Using Layer 4 NAT Mode ........................................ 14
   Overview .............................................................................. 14
   Load Balancer Configuration .................................................. 14
   Configure the Network Interfaces ............................................. 14
   Configure the Virtual Service (VIP) ......................................... 15
   Configure the Real Servers (RIPs) ............................................ 16
   Create a Floating IP to use for the eCopy ShareScan server server’s Default Gateway ........................................ 17
   eCopy ShareScan Server Configuration .................................... 17
   Default Gateway .................................................................... 17
   NAT Mode – Key Points ....................................................... 17
   Configure ShareScan server registry settings ............................. 17
   Real Server (eCopy ShareScan) Health Checks ........................... 18
   Layer 4 .............................................................................. 18
   Server Feedback Agent ........................................................ 18
   Agent Download .................................................................... 19
   Starting the Agent ................................................................ 20
   Configuration ...................................................................... 21
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancer Transparency</td>
<td>21</td>
</tr>
<tr>
<td>Layer 4</td>
<td>21</td>
</tr>
<tr>
<td>10. Testing &amp; Validation</td>
<td>21</td>
</tr>
<tr>
<td>Testing Load Balanced Services</td>
<td>21</td>
</tr>
<tr>
<td>Diagnosing VIP Connection Problems</td>
<td>22</td>
</tr>
<tr>
<td>Taking eCopy ShareScan servers Offline</td>
<td>23</td>
</tr>
<tr>
<td>Using Reports &amp; Log Files</td>
<td>23</td>
</tr>
<tr>
<td>11. Technical Support</td>
<td>24</td>
</tr>
<tr>
<td>12. Further Documentation</td>
<td>24</td>
</tr>
<tr>
<td>13. Conclusion</td>
<td>24</td>
</tr>
<tr>
<td>14. Appendix</td>
<td>25</td>
</tr>
<tr>
<td>Solving the ARP Problem</td>
<td>25</td>
</tr>
<tr>
<td>Configuring HA - Adding a Slave Appliance</td>
<td>29</td>
</tr>
<tr>
<td>15. Document Revision History</td>
<td>33</td>
</tr>
</tbody>
</table>
1. About this Guide

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

- eCopy ShareScan v6.2 and later

5. eCopy ShareScan

eCopy ShareScan 6.2 is an MFP document capture solution that enables MFP users to engage their business systems and processes by completely automating document capture processes. As a result, eCopy ShareScan simplifies MFP capture workflows and enables users with advanced imaging capabilities. The eCopy ShareScan software extends the capabilities of digital copiers and scanners. When installing and setting up a ShareScan system, you must be familiar with the scanning devices that you will use with ShareScan, the ShareScan software components, and the basic installation and configuration workflow.

6. Load Balancing eCopy ShareScan

Note

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

The Basics

The primary function of the load balancer is to distribute inbound requests across multiple eCopy ShareScan servers. This allows administrators to configure multiple servers and easily share the load between them. Adding additional capacity as demand grows then becomes straight forward and can be achieved by simply adding additional eCopy ShareScan servers to the load balanced cluster.

Ports & Protocols

The following table shows the ports that are normally used with eCopy ShareScan:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>TCP</td>
<td>Testing load balancer configuration</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Use</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>8080</td>
<td>TCP/HTTP</td>
<td>HTTP eCopy Tomcat application</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>HTTPS eCopy Tomcat application</td>
</tr>
<tr>
<td>9600</td>
<td>TCP</td>
<td>Web based MFDs</td>
</tr>
<tr>
<td>9261</td>
<td>TCP</td>
<td>Embedded MFDs i.e. Ricoh and Canon</td>
</tr>
</tbody>
</table>

**Note**

For the complete port list necessary to configure for a particular device vendor consult ShareScan documentation (High Availability and Load Balancing Deployment Guide, v6.2.)

**eCopy ShareScan Server Health-checks**

Regular eCopy ShareScan server monitoring ensures that failed servers are marked as down and client requests are only directed to functional servers. Health checks can range from a simple ICMP PING to a full negotiate check where content on a certain page is read and verified. Please refer to Real Server (eCopy ShareScan) Health Checks for more details.

**SSL Termination & Certificates**

It is recommended that all SSL traffic is terminated on the eCopy ShareScan servers (SSL pass-through).

**Persistence (aka Server Affinity)**

Source IP persistence is required when load balancing the eCopy ShareScan application and is the only available persistence method when load balancing at layer 4.

**Load Balancer Deployment**

The following diagram illustrates how the load balancer is deployed with multiple eCopy ShareScan servers.

![Load Balancer Deployment Diagram](image-url)

**VIP = Virtual IP Address**
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 Slave Appliance for more details on configuring a clustered pair.

Load Balancer Deployment Modes

The load balancer can be deployed in 4 fundamental ways: Layer 4 DR mode, Layer 4 NAT mode, Layer 4 SNAT mode and Layer 7 SNAT mode. For eCopy ShareScan, Layer 4 DR mode and Layer 4 NAT mode are recommended. These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode, please refer to Appliance & eCopy ShareScan Server Configuration – Using Layer 4 DR Mode, for configuring using NAT mode, refer to Appliance & eCopy ShareScan Server Configuration – 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 in DR mode i.e. having a different RIP port than the VIP port.
- DR mode is transparent, i.e. the Real Server will see the source IP address of the client.

Layer 4 NAT Mode
Layer 4 NAT mode is also 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:

  2-arm (using 2 Interfaces), 2 subnets (as shown above) - One interface on the load balancer is connected to subnet1 and the second interface and Real Servers are connected to subnet2. The VIP is brought up in subnet1. The default gateway on the Real Servers is set to be an IP address in subnet2 on the load balancer. Clients can be located in subnet1 or any remote subnet provided they can route to the VIP.

  2-arm (using 1 Interface), 2 subnets - same as above except that a single interface on the load balancer is allocated 2 IP addresses, one in each subnet.

  1-arm (using 1 Interface), 1 subnet - Here, the VIP is brought up in the same subnet as the Real Servers. For clients located in remote networks the default gateway on the Real Servers must be set to be an IP address on the load balancer. For clients located on the same subnet, return traffic would normally be sent directly to the client bypassing the load balancer which would break NAT mode. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer. For more 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.

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

• Port translation is possible in NAT mode, i.e. VIP:80 → RIP:8080 is possible.

### 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:

| Source | x.x.x.x:34567 | Destination | 10.0.0.20:80 |

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

| Source | x.x.x.x:34567 | Destination | 192.168.150:80 |

3) Replies return to the load balancer as:

| Source | 192.168.150:80 | Destination | x.x.x.x:34567 |

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

| Source | 10.0.0.20:80 | Destination | x.x.x.x:34567 |

### Loadbalancer.org Recommended Mode

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 eCopy ShareScan 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.

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 1 CPU, 2GB 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. 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.

Note
A number of compatibility issues have been found with various versions of Internet Explorer. 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>
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 & 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
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links

**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 slave unit is covered in Configuring HA - Adding a Slave Appliance.

8. Appliance & eCopy ShareScan Server Configuration – Using Layer 4 DR Mode

**Note**
It’s highly recommended that you have a working eCopy ShareScan environment first before implementing the load balancer and you must ensure that the DNS name points to the load balancer VIP.

**Overview**
This is our recommended deployment mode for eCopy ShareScan. It’s ideal when you want the fastest possible deployment and cannot make any network changes on the eCopy ShareScan servers.

**Load Balancer Configuration**

**Configure the Network Interface**
1. One interface is required. For more information on configuring network settings please refer to Initial Network Configuration.

**Configure the Virtual Service (VIP)**
1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Virtual Services and click Add a New Virtual Service.
2. Enter the following details:
3. Enter an appropriate name (Label) for the VIP, e.g. eCopy VIP.

4. Set the Virtual Service IP address field to the required IP address, e.g. 172.24.11.34.

5. Set the Virtual Service Ports field to *.

6. Leave Protocol set to TCP.

7. Ensure that Forwarding Method is set to Direct Routing.

8. Click Update.

9. Now click Modify next to the newly created Virtual Service.

10. Set Balance Mode (the load balancing algorithm) according to your requirements. "Weighted least connection" is the default and recommended method.

11. Persistence is enabled by default for new layer 4 VIPs and is based on source IP address. The persistence timeout can be set using the Persistence Timeout field, the default is 5 minutes which is normally fine for HTTP/HTTPS traffic.

12. Set the Health Checks Check type menu to Negotiate.

13. Set Check Port to 443.

14. Set Protocol to HTTPS.

15. Empty out the fields of Request to send and Response expected.

16. Click Update.

**Note**

For eCopy health check you can either monitor ports 8080 or 443 for the Tomcat service (Konica Minolta) or, ports 9600 for web-based devices or 9261 for embedded devices, like Ricoh and Canon as per the table in Ports & Protocols.

**Configure the Real Servers (RIPs)**

1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Real Servers and click Add a new Real Server next to the newly created Virtual Service.
2. Enter the following details:

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

3. Enter an appropriate name (Label) for the first eCopy ShareScan server, e.g. ShareScan1.
4. Change the *Real Server IP Address* field to the required IP address, e.g. 172.24.11.32.
5. Leave other settings at their default values.
6. Click *Update*.
7. Repeat the above steps for your other eCopy ShareScan server(s).

**eCopy ShareScan Server Configuration**

**Solve the 'ARP Problem'**

As mentioned previously, DR mode works by changing the destination MAC address of the incoming packet to match the selected ShareScan server on the fly which is very fast. When the packet reaches the ShareScan server it expects the ShareScan server to own the Virtual Services IP address (VIP). This means that you need to ensure that the ShareScan server (and the load balanced application) respond to both the ShareScan servers own IP address and the VIP. The ShareScan server should not respond to ARP requests for the VIP. Only the load balancer should do this.

To achieve this, a loopback adapter is added to the ShareScan servers. The IP address is set to be the same as the Virtual Service and the loopback adapter is configured so that it does not respond to ARP requests. Please refer to *Solving the ARP Problem* for full details of solving the ARP problem for Windows 2012 & later.

**DR Mode – Key Points**

- You must solve the ‘ARP Problem’ on all eCopy ShareScan servers in the cluster (please refer to *Solving the ARP Problem* for more information)

- Virtual Services & Real Servers (i.e. the eCopy ShareScan servers) must be within the same switch fabric. They can be on different subnets but this cannot be across a router – this is due to the way DR mode works, i.e. by changing MAC addresses to match the destination server

- Port translation is not possible, e.g. VIP:80 → eCopy ShareScan:82 is not allowed. The port used for the VIP & RIP must be the same
Configure ShareScan server registry settings
The following registry changes should be made on the ShareScan servers:

1. Using the Start menu, enter `regedit` to access the registry.

2. Open/expand the tree on the left pane and select 
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance\ShareScan`.

3. In the right pane, choose the string `ManagerIP`. Double click on it and enter the IP address of the load balancer VIP.

4. Next, right click on the right side pane and select "new string". Name the new string value as `ClusterNodeIP`. Double click on the new string and enter the IP address of the main network adapter, i.e. the real server IP address.

5. In the left pane, now navigate to `ShareScanManager`. In the right pane, right click and choose `New String` and enter the name `ClusterName`.

6. Double click on `ClusterName` and change the value to the FQDN of the load balancer VIP and click `OK`.

7. Reboot the server to apply the registry changes.

9. Appliance & eCopy ShareScan Server Configuration – Using Layer 4 NAT Mode

   **Note**
   It's highly recommended that you have a working eCopy ShareScan environment first before implementing the load balancer.

**Overview**
If the load balancer and the eCopy ShareScan servers are not part of the same layer 2 network, then DR mode cannot be used. If you require a high performance solution that is transparent by default (i.e. the client IP address is maintained through the load balancer) then layer 4 NAT mode can be used. Layer 4 NAT mode is also a high performance solution, although not as fast as layer 4 DR mode. This is because eCopy ShareScan server responses must flow back to the client via the load balancer rather than directly as with DR mode.

**Load Balancer Configuration**

**Configure the Network Interfaces**
1. To configure the first network interface, please refer to **Initial Network Configuration**.

2. Using the WebUI, navigate to: Local Configuration > Network Interface Configuration.

3. Define an additional IP address in a different subnet – either by using 2 separate interfaces as shown below or by using a single interface with an additional alias (secondary) address.
Configure the Virtual Service (VIP)

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

2. Enter the following details:

   - **Label**: Enter an appropriate name (Label) for the VIP, e.g. *eCopy NAT VIP*.
   - **Virtual Service IP address**: Set the Virtual Service IP address field to the required IP address, e.g. *192.168.86.134*.
   - **Virtual Service Ports**: Set the Virtual Service Ports field to *.
   - **Protocol**: Leave Protocol set to TCP.
   - **Forwarding Method**: Set the Forwarding Method to NAT.

3. Enter an appropriate name (Label) for the VIP, e.g. *eCopy NAT VIP*.

4. Set the Virtual Service IP address field to the required IP address, e.g. *192.168.86.134*.

5. Set the Virtual Service Ports field to *.

6. Leave Protocol set to TCP.

7. Set the Forwarding Method to NAT.

8. Click Update.
9. Now click **Modify** next to the newly created Virtual Service.

10. Set **Balance Mode** (the load balancing algorithm) according to your requirements. "Weighted least connection" is the default and recommended method.

11. Persistence is enabled by default for new layer 4 VIPs and is based on source IP address. The persistence timeout can be set using the **Persistence Timeout** field, the default is 5 minutes which is normally fine for HTTP/HTTPS traffic.

12. Set the **Health Checks Check type** menu to **Negotiate**.

13. Set **Check Port** to **443**.

14. Set **Protocol** to **HTTPS**.

15. Ensure that the fields **Request to send** and **Response expected** are blank.

16. Click **Update**.

**Note**

For eCopy health check you can either monitor ports 8080 or 443 for the Tomcat service (Konica Minolta) or, ports 9600 for web-based devices or 9261 for embedded devices, like Ricoh and Canon as per the table in **Ports & Protocols**.

**Configure the Real Servers (RIPs)**

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

2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>ShareScan1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>172.24.11.32</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

3. Enter an appropriate name (Label) for the first eCopy ShareScan server, e.g. **ShareScan1**.

4. Change the **Real Server IP Address** field to the required IP address, e.g. **172.24.11.32**.

5. Leave the **Real Server Port** blank.

6. Leave other settings at their default values.

7. Click **Update**.
8. Repeat the above steps for your other eCopy ShareScan server(s).

Create a Floating IP to use for the eCopy ShareScan server server's Default Gateway

The default gateway on each eCopy ShareScan server server must be configured to be an IP address on the load balancer. It’s possible to use the IP address assigned to the internal facing interface (eth0 in this example) for the default gateway, although it’s recommended that an additional floating IP is created for this purpose. This is required if two load balancers (our recommended configuration) are used. In this scenario if the master unit fails, the floating IP will be brought up on the slave.

To create a floating IP address on the load balancer:

1. Using the WebUI, navigate to: Cluster Configuration > Floating IPs.
2. Enter the required IP address to be used for the default gateway, e.g. 172.24.11.35.
3. Click Update.

Once added, there will be two floating IP’s, one for the Virtual Service (192.168.86.134) and one for the default gateway (e.g. 172.24.11.35) as shown below:

<table>
<thead>
<tr>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.24.11.35</td>
</tr>
<tr>
<td>192.168.86.134</td>
</tr>
</tbody>
</table>

Once added, there will be two floating IP’s, one for the Virtual Service (192.168.86.134) and one for the default gateway (e.g. 172.24.11.35) as shown below:

**eCopy ShareScan Server Configuration**

**Default Gateway**

To ensure return traffic passes back to the client via the load balancer, set the default gateway of each eCopy ShareScan server to be the floating IP address added in the previous step, in this example 172.24.11.35.

**NAT Mode – Key Points**

- Virtual Services & Real Servers (i.e. the eCopy ShareScan servers) must be on different subnets
- The default gateway on the eCopy ShareScan servers should be an IP address on the load balancer (for an HA pair this must be a floating IP address)
- Port translation is possible, e.g. VIP:80 → RIP:8080 is allowed

**Configure ShareScan server registry settings**

The following registry changes should be made on the ShareScan servers:

1. Using the Start menu, enter regedit to access the registry.
2. Open/expand the tree on the left pane and select HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance\ShareScan.
3. In the right pane, choose the string ManagerIP. Double click on it and enter the IP address of the load balancer VIP.

4. Next, right click on the right side pane and select "new string". Name the new string value as ClusterNodeIP. Double click on the new string and enter the IP address of the main network adapter, i.e. the real server IP address.

5. In the left pane, now navigate to ShareScanManager. In the right pane, right click and choose New String and enter the name ClusterName.

6. Double click on ClusterName and change the value to the FQDN of the load balancer VIP and click OK.

7. Reboot the server to apply the registry changes.

Real Server (eCopy ShareScan) Health Checks

The load balancer performs regular health checks to ensure that each server in the cluster is healthy and able to accept client connections. The health check options at layer 4 have been outlined below.

Layer 4
By default, a TCP connect health check is used for newly created layer 4 Virtual Services. The following tables lists all options available:

<table>
<thead>
<tr>
<th>Check Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negotiate</td>
<td>Sends a request and looks for a specific response. This option enables the load balancer to perform a more robust check. For example, an HTTP check can be configured that requests a certain page and then looks for a specific word on that page.</td>
</tr>
<tr>
<td>Connect to port</td>
<td>Just do a simple connect to the specified port/service &amp; verify that it’s able to accept a connection.</td>
</tr>
<tr>
<td>Ping server</td>
<td>Sends an ICMP echo request packet to the Real Server.</td>
</tr>
<tr>
<td>External check</td>
<td>Use a custom script for the health check.</td>
</tr>
<tr>
<td>No checks, always Off</td>
<td>All Real Servers are off.</td>
</tr>
<tr>
<td>No checks, always On</td>
<td>All Real Servers are on (no checking).</td>
</tr>
<tr>
<td>5 Connects, 1 Negotiate</td>
<td>Do 5 connect checks and then 1 negotiate check.</td>
</tr>
<tr>
<td>10 Connects, 1 Negotiate</td>
<td>Do 10 connect checks and then 1 negotiate check.</td>
</tr>
</tbody>
</table>

Note: For full details on the options available, please refer to Real Server Health Monitoring & Control.

Server Feedback Agent
The load balancer can modify the weight (amount of traffic) of each server by gathering data from either a custom agent or an HTTP server. For layer 4 VIPs the feedback method can be set to either agent or HTTP, for Layer 7 VIPs, only the agent method is supported.

A telnet to port 3333 on a Real Server with the agent installed will return the current idle stats as an integer value in the range 0 – 100. The figure returned can be related to CPU utilization, RAM usage or a combination of both. This can be configured using the XML configuration file located in the agents installation folder (by default C:\ProgramData\LoadBalancer.org\LoadBalancer).
The load balancer typically expects a 0-99 integer response from the agent which by default relates to the current CPU idle state, e.g. a response of 92 would imply that the Real Servers CPU is 92% idle. The load balancer will then use the formula \((92/100 \times \text{requested_weight})\) to find the new optimized weight.

**Note**

The ‘Requested Weight’ is the weight set in the WebUI for each Real Server. For more information please also refer to this blog.

**Agent Download**

The latest Windows feedback agent can be downloaded from [here](#). To install the agent, run `loadbalanceragent.msi` on each eCopy ShareScan Server:

Leave the default location or change according to your requirements, click **Next**.
Leave the default location or change according to your requirements, click Next.

Click Install to start the installation process.

Click Finish.

**Note** The agent should be installed on all eCopy ShareScan Servers in the cluster.

**Starting the Agent**

Once the installation has completed, you'll need to start the service on the Real Servers. The service is controlled by the Feedback Agent monitor & control program that is also installed along with the Agent. This can be accessed on the Windows server from: Start> Loadbalancer.org > Loadbalancer.org Feedback Agent. It's also possible to start the service using the services snap-in – the service is called 'LBCPUMon'.
To start the service, click the **Start** button.

To stop the service, click the **Stop** button.

### Configuration

To Configure Virtual Services to use the feedback agent, follow the steps below:

1. Using the WebUI, navigate to:
   
   *Cluster Configuration > Layer 4 Virtual Services*

2. Click **Modify** next to the Virtual Service.

   ![Configuration Interface]

3. Change the Feedback Method to **Agent**.

4. Click **Update**.

5. Reload/Restart services as prompted.

### Load Balancer Transparency

**Layer 4**

Both Layer 4 DR mode and layer 4 NAT mode are transparent by default. This means that ShareScan will log the actual IP address of the client rather than the IP address of the load balancer.

### 10. Testing & Validation

**Testing Load Balanced Services**

eCopy ShareScan has an application troubleshooting tool that can be utilised to test connectivity via the load balancer VIP to the eCopy Sharescan real servers. As such, to initiate the troubleshooter follow the defined steps below.
1. Start ShareScan Troubleshooter on all Sharescan server nodes and one Sharescan client that has access to the Sharescan load balanced VIP.

2. On the ShareScan server nodes click the Advanced drop down menu > Network tests > Server side network test. It will automatically start listening on port 9600.

3. On the non-load balanced client PC click the Advanced drop down menu > Network tests > Client side network test.

4. Enter the ShareScan Virtual IP into the Server address / hostname, and click Connect.

5. The request should now connect to one of the Sharescan servers via the load balancer VIP resulting in a connection message in one of the open dialogues on one of the servers.

6. Confirm that the IP shown by the connection message is the IP of the is of the client PC and NOT the IP of the load balancer.

**Why test using two clients?** If you use a single client it will most likely keep on hitting the same server for multiple requests. This is to do with the way that the load balancing algorithms are optimized.

**Diagnosing VIP Connection Problems**

1. **Make sure that the device is active** - this can be checked in the WebUI. For a single appliance, the status bar should report Master & Active as shown below:

   ![Master Status](image)

2. **Check that the VIP / floating IP is up** - Using View Configuration > Network Configuration verify that the VIP is active on the load balancer, if not check Logs > Heartbeat for errors.

   ```
   2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
   link/ether 00:0c:29:cf:18:03 brd ff:ff:ff:ff:ff:ff
   inet 192.168.110.85/18 brd 192.168.127.255 scope global eth0
     valid_lft forever preferred_lft forever
   inet 192.168.110.90/18 brd 192.168.127.255 scope global secondary eth0
     valid_lft forever preferred_lft forever
   ```

   The above example shows that the interface address (192.168.110.85) and the VIP address (192.168.110.90) are both up.

3. **Check that the eCopy ShareScan Servers are up** - Using System Overview make sure that none of your VIPs are colored red. If they are, the entire cluster is down (i.e. all eCopy ShareScan Servers). Green indicates a healthy cluster, yellow indicates that your cluster may need attention (one or more of the eCopy ShareScan Servers may be down), and blue indicates all eCopy ShareScan Server have been deliberately taken offline (by using either Halt or Drain).
4. Check the connection state -

For Layer 4 DR mode VIPs check *Reports > Layer 4 Current Connections* to view the current traffic in detail. Any packets with state **SYN_RECV** imply that the 'ARP Problem' has not been correctly solved on the eCopy ShareScan Servers. Please refer to *Solving the ARP Problem* for more details on solving the ARP problem.

For layer 4 NAT mode VIPs check *Reports > Layer 4 Current Connections* to view the current traffic in detail. Any packets with state **SYN_RECV** often imply that the default gateway on the eCopy ShareScan Servers has not been set to be an IP address on the load balancer.

Taking eCopy ShareScan servers Offline

1. Using the *System Overview* check that when you Halt one of the eCopy ShareScan Servers the connections are redirected to the other server in the cluster.

2. Remove the network cable from one of the eCopy ShareScan servers or stop the web service/process, wait a few seconds (for the load balancer to detect the change) and then refresh the browsers on both clients. They should now both switch to the same server (since one has been removed from the load balancing list). Also check that the server is shown red (down) in the system overview.

3. Replace the network cable, wait a few seconds and then refresh the browsers again. After a few refreshes they should again show different web servers. Also check that the server is shown green (up) in the system overview.

The *System Overview* will also show the updated status as these tests are performed:

![System Overview Table](image)

- **RIP1** is green. This indicates that it’s operating normally.

- **RIP2** is blue. This indicates that it has been either Halted or Drained. In this example Halt has been used as indicated by **Online (Halt)** being displayed. If it had been drained it would show as **Online (Drain)**.

- **RIP3** is red. This indicates that it has failed a health check.

Using Reports & Log Files

The appliance includes several logs and reports that are very useful when diagnosing issues. Both are available as main menu options in the WebUI. For more details, please refer to *Appliance Monitoring*.
11. Technical Support

If you have any questions regarding the appliance or would like assistance designing your deployment, please don’t hesitate to contact our support team: support@loadbalancer.org.

12. Further Documentation


13. Conclusion

Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced Kofax eCopy ShareScan environments.
14. Appendix

Solving the ARP Problem

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

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:

   ![Loopback Properties](image)

   **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:

```plaintext
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:

```plaintext
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:

```plaintext
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:

```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:
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 Slave 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 Slave should be added. Once the Primary and Slave are paired, all load balanced services configured on the Primary are automatically replicated to the Slave 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 Slave. 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 Slave) will take over.

A number of settings are not replicated as part of the Primary/Slave pairing process and therefore must be manually configured on the Slave 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 Slave node - i.e. create a highly available clustered pair:

1. Deploy a second appliance that will be the Slave 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 Slave (peer) appliance as shown above.

4. Click **Add new node**.

5. The pairing process now commences as shown below:

![Create a Clustersed Pair](image)

6. Once complete, the following will be displayed:

![High Availability Configuration - master](image)

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 Slave appliance.

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>27 November 2019</td>
<td>Initial draft</td>
<td>Initial draft</td>
<td>IBG, AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>20 December 2019</td>
<td>Guide update</td>
<td>Health checks updated</td>
<td>IBG</td>
</tr>
<tr>
<td>1.0.2</td>
<td>9 March 2020</td>
<td>Guide update</td>
<td>Health checks updated</td>
<td>IBG</td>
</tr>
<tr>
<td>1.0.3</td>
<td>3 September 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</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.