

# Load Balancing DataCore Swarm Gateway

Version 1.0.0



# **Table of Contents**

I. About this Briet	
2. Loadbalancer.org Appliances Supported	
3. Software Versions Supported	
3.1. Loadbalancer.org Appliance	
3.2. DataCore Swarm Gateway	
4. DataCore Swarm Gateway	
5. Load Balancing DataCore Swarm Gateway	
5.1. Persistence (aka Server Affinity)	
5.2. Virtual Service (VIP) Requirements	
5.3. Port Requirements	
6. Deployment Concept	
7. Load Balancer Deployment Methods	4
7.1. Layer 4 DR Mode	
7.2. Layer 7 SNAT Mode	
7.3. Our Recommendation	
8. Configuring DataCore Swarm Gateway for Load Balancing	
8.1. Solving the ARP Problem for Linux	
Method 1: ARP Behaviour and Loopback Interface Changes	
Method 2: NAT "redirect" via iptables	
Method 3: NAT "redirect" via nftables	
Method 4: NAT "redirect" via firewall-cmd	
9. Loadbalancer.org Appliance – the Basics	
9.1. Virtual Appliance	
9.2. Initial Network Configuration	
9.3. Accessing the Appliance WebUI	
Main Menu Options	
9.4. Appliance Software Update	
Determining the Current Software Version	
Checking for Updates using Online Update.	
Using Offline Update	
9.5. Ports Used by the Appliance	
9.6. HA Clustered Pair Configuration	
10. Appliance Configuration for DataCore Swarm Gateway – Using Layer 4 DR Mode	
10.1. Configuring the Virtual Service (VIP).	
10.2. Defining the Real Servers (RIPs)	
11. Appliance Configuration for DataCore Swarm Gateway – Using Layer 7 SNAT Mode	
11.1. Configuring the Virtual Service (VIP).	
11.2. Defining the Real Servers (RIPs)	
11.3. Finalizing the Layer 7 Configuration	
12. Testing & Verification	
12.1. Using System Overview.	
13. Technical Support	
14. Further Documentation	
15. Appendix	
15.1. Configuring HA - Adding a Secondary Appliance	
Non-Replicated Settings	
Adding a Secondary Appliance - Create an HA Clustered Pair	
16. Document Revision History	

### 1. About this Brief

This brief outlines the steps required to configure a load balanced DataCore Swarm Gateway environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any DataCore Swarm Gateway 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 DataCore Swarm Gateway. 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. Software Versions Supported

#### 3.1. Loadbalancer.org Appliance

V8.6.1 and later

**f** 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.

# 3.2. DataCore Swarm Gateway

All versions

# 4. DataCore Swarm Gateway

DataCore Swarm provides an on-premises object storage solution allowing S3/HTTP access to any application, device, or end-user. These services are presented via *gateway* servers. These gateways need to be load balanced in order to provide highly available and resilient service access.

# 5. Load Balancing DataCore Swarm Gateway

8 Note

It's highly recommended that you have a working DataCore Swarm Gateway environment first before implementing the load balancer.

# 5.1. Persistence (aka Server Affinity)

DataCore Swarm Gateways require source IP address-based persistence to be applied. This ensures that a given client will "stick" to the same gateway server for the duration of their session.



#### 5.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for DataCore Swarm Gateway, the following VIP is required:

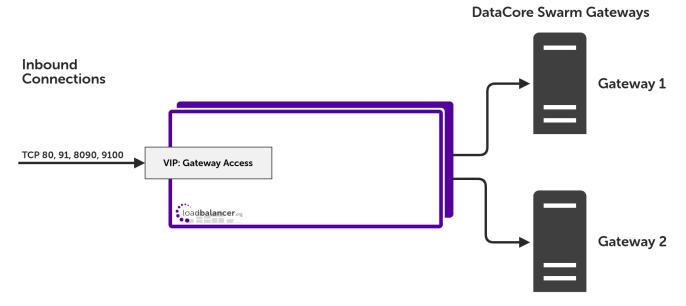
Gateway Access

#### 5.3. Port Requirements

The following table shows the ports that are load balanced:

Ports	Protocols	Use
80, 91, 8090, 9100	TCP	Access to Gateway Services

# 6. Deployment Concept



VIPs = Virtual IP Addresses

8 Note

The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to the section Configuring HA - Adding a Secondary Appliance in the appendix for more details on configuring a clustered pair.

# 7. Load Balancer Deployment Methods

The load balancer can be deployed in 4 fundamental ways: Layer 4 DR mode, Layer 4 NAT mode, Layer 4 SNAT mode, and Layer 7 SNAT mode.

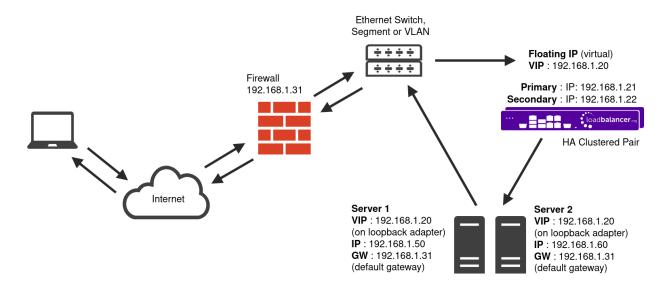
For DataCore Swarm Gateway, using layer 4 DR mode is recommended. It it also possible to use layer 7 SNAT mode, however the raw performance of this set up is not as great as layer 4 DR mode. These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode please refer to Section 10, "Appliance Configuration for DataCore Swarm Gateway – Using Layer 4 DR Mode", and for configuring using layer 7 SNAT mode refer to Section 11, "Appliance Configuration for DataCore Swarm

#### 7.1. Layer 4 DR Mode

One-arm direct routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.

8 Note

Kemp, Brocade, Barracuda & A10 Networks call this Direct Server Return and F5 call it nPath.

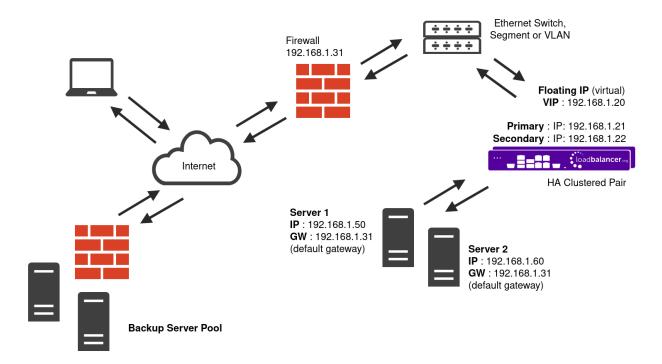


- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that you need to ensure that the 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.

# 7.2. 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.



- 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 mode-specific 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.

#### 7.3. Our Recommendation

Layer 4 DR mode is the recommended deployment method. It offers the greatest raw performance and is particularly well suited to read-intensive storage scenarios.

Layer 7 SNAT mode is the simplest and most flexible solution. It **must** be used if the gateway servers are on a different network segment to the load balancers (no layer 2 connectivity between them) or when it is not possible

# 8. Configuring DataCore Swarm Gateway for Load Balancing

If layer 7 SNAT mode is used then this section can safely be ignored and skipped.

If layer 4 DR mode is used then the 'ARP problem' must be solved. This involves configuring each real server (each DateCore Swarm Gateway in this context) to be able to receive traffic destined for the VIP address, and ensuring that each real server does not respond to ARP requests for the VIP address – only the load balancer should do this. Instructions on how to do this are as follows.

#### 8.1. Solving the ARP Problem for Linux

There are two different approaches on how to configure a Linux server for correct operation when DR mode load balancing is in use:

- Modifying the server's ARP behaviour and adding the relevant VIP addresses to the loopback interface
- Using NAT to convince the server to accept and reply to packets addressed to the relevant VIP addresses

Four independent methods are described below along with instructions. Each method follows one of the two approaches above. The specific method chosen will depend on technical requirements, the Linux distribution in use, and personal preferences.

The first method involves setting kernel parameters to alter the server's ARP behaviour and adding IP addresses to the loopback interface. This method should be universally applicable to any Linux server **making this the preferred method**.

If setting kernel parameters and adding IP addresses is not possible for some reason, the remaining three methods describe setting up a server for DR mode operation by using NAT via the **redirect** target/statement. The specific instructions depend on the packet filtering framework and tooling in use, which varies between Linux distributions. Methods are presented for iptables, nftables, and the **firewall-cmd** tool.

#### Method 1: ARP Behaviour and Loopback Interface Changes

This is the preferred method as it should be applicable to any Linux server and doesn't require any additional packet filtering or NAT considerations.

Each real server needs the loopback interface to be configured with the virtual IP addresses (VIPs) of the relevant load balanced services. This is often just a single VIP address, but the logic described below can be extended to cover multiple VIPs on a server. Having the VIPs on the loopback interface allows the server to accept inbound load balanced packets that are addressed to a VIP.

The server **must not** respond to ARP requests for the VIP addresses. The server also **must not** use ARP to announce the fact that it owns the VIP addresses. This is necessary to prevent IP address conflicts, as *all* of the real servers *and* the load balancer will own the VIP addresses. Only the load balancer should announce ownership of the VIPs.

To configure the behaviour described above, follow all of the steps below on each real server.

#### Step 1 of 4: Re-configuring ARP behaviour

This step is only applicable if IPv4-based virtual services are in use.

Add the following lines to the file /etc/sysctl.conf (create this file if it does not already exist):

```
net.ipv4.conf.all.arp_ignore=1
net.ipv4.conf.eth0.arp_ignore=1
net.ipv4.conf.eth1.arp_ignore=1
net.ipv4.conf.all.arp_announce=2
net.ipv4.conf.eth0.arp_announce=2
net.ipv4.conf.eth1.arp_announce=2
```

Adjust the commands shown above to suit the server's network configuration, e.g. a different number of network interfaces or a different interface naming convention.

For reference, the effect of these kernel parameter changes on the server is as follows:

8 Note

- arp\_ignore=1: This configures the server to only reply to an ARP request if the request's
  target IP address is local to the incoming interface. This can never be true for VIP
  addresses on the loopback interface, as the loopback interface can never be an incoming
  interface for ARP requests from other devices. Hence, ARP requests for VIP addresses are
  always ignored.
- arp\_announce=2: This prevents the server from sending an ARP request out of an interface A where the ARP request's sender/source address is stated to be an IP address that is local to some other interface B. For example, this prevents the server from sending an ARP request from a VIP address (which is local to the loopback interface) out of eth0, which would announce that the server owns the VIP address.

#### Step 2 of 4: Re-configuring duplicate address detection (DAD) behaviour

This step is only applicable if IPv6-based virtual services are in use.

Add the following lines to the file /etc/sysctl.conf (create this file if it does not already exist):

```
net.ipv6.conf.lo.dad_transmits=0
net.ipv6.conf.lo.accept_dad=0
```

For reference, the effect of these kernel parameter changes on the server is as follows:

8 Note

- dad\_transmits=0: This prevents a given interface from sending out duplicate address
  detection probes in order to test the uniqueness of unicast IPv6 addresses. Any IPv6 VIP
  addresses will not be unique, so this mechanism is disabled.
- accept\_dad=0: This prevents a given interface from accepting duplicate address
  detection messages. This prevents any IPv6 VIP addresses from being marked as
  duplicate addresses.

#### Step 3 of 4: Applying the new settings

To apply the new settings, either reboot the real server or execute the following command to immediately apply the changes:

```
/sbin/sysctl -p
```

Steps 1, 2, and 3 can be replaced by instead modifying the necessary kernel variables by writing directly to their corresponding files under /proc/sys/. Note that changes made in this way will not persist across reboots.

Execute the following commands (as root) to implement these temporary changes (adapting the number of interfaces and interface names as needed):

8 Note

```
echo 1 > /proc/sys/net/ipv4/conf/all/arp_ignore
echo 1 > /proc/sys/net/ipv4/conf/eth0/arp_ignore
echo 1 > /proc/sys/net/ipv4/conf/eth1/arp_ignore
echo 2 > /proc/sys/net/ipv4/conf/all/arp_announce
echo 2 > /proc/sys/net/ipv4/conf/eth0/arp_announce
echo 2 > /proc/sys/net/ipv4/conf/eth1/arp_announce
echo 0 > /proc/sys/net/ipv6/conf/lo/dad_transmits
echo 0 > /proc/sys/net/ipv6/conf/lo/accept_dad
```

#### Step 4 of 4: Adding the virtual IP addresses (VIPs) to the loopback interface

Each of the VIP addresses must be permanently added to the loopback interface. VIPs must be added with a network prefix of /32 for IPv4 addresses or /128 for IPv6 addresses. The IP addresses can be added using the usual configuration files and tools for modifying network interfaces, which vary between different Linux distributions.

As an alternative, the ip command can be used as a universal way to add IP addresses to any Linux server. Note that addresses added in this way will not persist across reboots. To make these addresses permanent, add the ip commands to an appropriate startup script such as /etc/rc.local.

Execute the following ip command for each IPv4 VIP:

```
ip addr add dev lo <IPv4-VIP>/32
```

Execute the following ip command for each IPv6 VIP:

```
ip addr add dev lo <IPv6-VIP>/128
```

To check that the VIPs have been successfully added, execute the command:

```
ip addr ls
```

To remove an IPv4 VIP from the loopback adapter, execute the command:

```
ip addr del dev lo <IPv4-VIP>/32
```

To remove an IPv6 VIP from the loopback adapter, execute the command:

```
ip addr del dev lo <IPv6-VIP>/128
```

#### Method 2: NAT "redirect" via iptables

iptables can be used on each real server to identify incoming packets that are addressed to a virtual IP address (VIP) and redirect those packets to the server itself. This is achieved using the **REDIRECT** target in iptables, which performs the necessary NAT to make this possible. This allows a real server to accept packets addressed to a VIP without the server owning the VIP.

Execute the following command to put the necessary iptables rule in place to redirect traffic for a single IPv4 VIP address. Note that iptables rules added in this way *will not persist across reboots*. To make such a rule permanent, either add the rule to an iptables firewall script, if one is provided with the Linux distribution in question, or add the command to an appropriate startup script such as /etc/rc.local on each real server.

```
iptables -t nat -A PREROUTING -d <IPv4-VIP> -j REDIRECT
```

The VIP address should be changed to match the virtual service in question, for example:

```
iptables -t nat -A PREROUTING -d 10.0.0.21 -j REDIRECT
```

The example above will redirect any incoming packets destined for 10.0.0.21 (the virtual service) locally, i.e. to the primary address of the incoming interface on the real server.

If a real server is responsible for serving *multiple* VIPs then additional iptables rules should be added to cover each VIP.

For an IPv6 VIP address, a command like the following should be used:

```
ip6tables -t nat -A PREROUTING -d <IPv6-VIP> -j REDIRECT
```

The VIP address should be changed to match the virtual service in question, for example:

```
ip6tables -t nat -A PREROUTING -d 2001:db8::10 -j REDIRECT
```

**8** Note

Method 2 may not be appropriate when using IP-based virtual hosting on a web server. This is because an iptables **REDIRECT** rule will redirect incoming packets to the *primary address* of the incoming interface on the web server rather than any of the virtual hosts that are configured.



#### Method 3: NAT "redirect" via nftables

nftables is the modern Linux kernel packet filtering framework. It is supported on all major Linux distributions and has replaced iptables as the default framework on most major distributions.

nftables can be used on each real server to identify incoming packets that are addressed to a virtual IP address (VIP) and redirect those packets to the server itself. This is achieved using the **redirect** statement in nftables, which performs the necessary NAT to make this possible. This allows a real server to accept packets addressed to a VIP without the server owning the VIP.

Use a script like the following to put the necessary nftables structures in place to redirect traffic for both IPv4 and IPv6 VIP addresses. To make such a configuration permanent, either add the **inet nat** table to an nftables firewall script, if one is provided with the Linux distribution in question, or configure a script like the following to execute as a startup script on each real server.

```
#!/usr/sbin/nft -f

table inet nat {
    chain prerouting {
        comment "Allow server to accept packets destined for VIP addresses";
        type nat hook prerouting priority -100; policy accept;
        ip daddr <IPv4-VIP> redirect comment "Description"
        ip6 daddr <IPv6-VIP> redirect comment "Description"
    }
}
```

The VIP addresses and comments should be changed to match the virtual services in question, for example:

```
#!/usr/sbin/nft -f

table inet nat {
    chain prerouting {
        comment "Allow server to accept packets destined for VIP addresses";
        type nat hook prerouting priority -100; policy accept;
        ip daddr 10.0.0.21 redirect comment "VIP 1: HTTP"
        ip6 daddr 2001:db8::10 redirect comment "VIP 2: HTTPS"
    }
}
```

The example above will redirect any incoming packets destined for 10.0.0.21 or 2001:db8::10 (the virtual services) locally, i.e. to the primary address of the incoming interface (for each IP version) on the real server.

Note that **Linux kernels prior to 5.2** may not support performing NAT (which is required for the **redirect** statement) in an inet family table. In this scenario, use either an ip or an ip6 family table instead, or both if a mixture of IPv4 and IPv6 VIPs are in use on the same server. Also note that older kernels may not support the use of comments in chains.

Note that Linux kernels prior to 4.18 require explicitly registering both prerouting and postrouting chains in order



for the implicit NAT of the **redirect** statement to be correctly performed in both the inbound and outbound directions.

A legacy-friendly setup may look like the following:

```
#!/usr/sbin/nft -f
table ip nat {
   chain prerouting {
       type nat hook prerouting priority -100; policy accept;
        ip daddr 10.0.0.21 counter redirect comment "VIP 1: HTTP"
   chain postrouting {
        type nat hook postrouting priority 100; policy accept;
}
table ip6 nat {
    chain prerouting {
        type nat hook prerouting priority -100; policy accept;
        ip6 daddr 2001:db8::10 counter redirect comment "VIP 2: HTTPS"
    }
   chain postrouting {
        type nat hook postrouting priority 100; policy accept;
   }
}
```

8 Note

Method 3 may not be appropriate when using IP-based virtual hosting on a web server. This is because an inftables **redirect** statement will redirect incoming packets to the *primary address* of the incoming interface on the web server rather than any of the virtual hosts that are configured. Where this is an issue, use method 1 instead.

#### Method 4: NAT "redirect" via firewall-cmd

Some recent versions of Linux distributions make use of firewalld as a high-level firewall configuration framework. In this case, while it may actually be iptables performing the work at a lower level, it may be preferred to implement the iptables NAT solution described in method 2 in firewalld, as opposed to directly manipulating iptables. This is achieved by using the firewall-cmd tool provided by firewalld and executing a command like the following on each real server:

```
firewall-cmd --permanent --direct --add-rule ipv4 nat PREROUTING 0 -d <IPv4-VIP> -j REDIRECT
```

The VIP address should be changed to match the virtual service in question, for example:

```
firewall-cmd --permanent --direct --add-rule ipv4 nat PREROUTING 0 -d 10.0.0.50 -j REDIRECT
```

To apply the new configuration, reload the firewall rules like so:



firewall-cmd --reload

Configuration applied in this way will be permanent and will persist across reboots.

8 Note

Method 4 may not be appropriate when using IP-based virtual hosting on a web server. This is because an iptables **REDIRECT** rule will redirect incoming packets to the *primary address* of the incoming interface on the web server rather than any of the virtual hosts that are configured. Where this is an issue, use method 1 instead.

# 9. Loadbalancer.org Appliance - the Basics

### 9.1. Virtual Appliance

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

The same download is used for the licensed product, the only difference is that a license key file

Note (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

Note

Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

The VA has 4 network adapters. For VMware only the first adapter (**eth0**) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

# 9.2. Initial Network Configuration

After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS Server and other network settings.

(1) Important Be sure to set a secure password for the load balancer, when prompted during the setup routine.

# 9.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

Note

There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

8 Note

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

1. Using a browser, navigate to the following URL:

#### https://<IP-address-configured-during-the-network-setup-wizard>:9443/lbadmin/

8 Note

You'll receive a warning about the WebUl's certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

2. Log in to the WebUI using the following credentials:

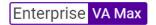
Username: loadbalancer

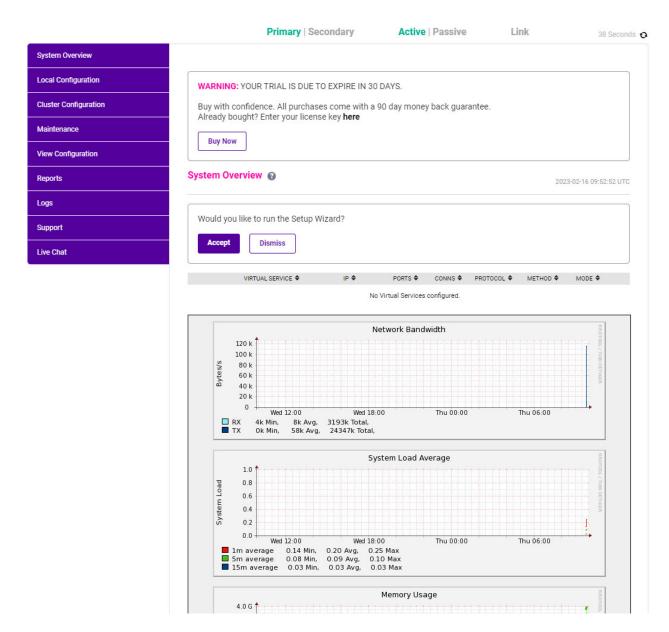
Password: <configured-during-network-setup-wizard>

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

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

LOADBALANCER





3. You'll be asked if you want to run the Setup Wizard. Click **Dismiss** if you're following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.

Note The Setup Wizard can only be used to configure Layer 7 services.

#### 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



### 9.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

#### **Determining the Current Software Version**

The software version is displayed at the bottom of the WebUI as shown in the example below:

Copyright © Loadbalancer.org Inc. 2002 - 2023 ENTERPRISE VA Max - v8.9.0



#### Checking for Updates using Online Update

Note

By default, the appliance periodically contacts the Loadbalancer.org update server and checks for updates. An update check can also be manually triggered as detailed below.

- 1. Using the WebUI, navigate to: *Maintenance > Software Update*.
- 2. Select Online Update.
- 3. If the latest version is already installed, a message similar to the following will be displayed:

Information: Version v8.9.0 is the current release. No updates are available

- 4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
- 5. Click **Online Update** to start the update process.
  - Note Do not navigate away whilst the update is ongoing, this may cause the update to fail.
- 6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

Information: Update completed successfully.

7. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

#### **Using Offline Update**

If the load balancer does not have access to the Internet, offline update can be used.



8 Note

Please contact support@loadbalancer.org to check if an update is available and obtain the latest offline update files.

#### To perform an offline update:

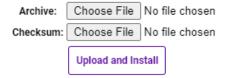
- 1. Using the WebUI, navigate to: *Maintenance > Software Update*.
- 2. Select Offline Update.
- 3. The following screen will be displayed:

#### **Software Update**

#### Offline Update

The following steps will lead you through offline update.

- Contact Loadbalancer.org support to obtain the offline update archive and checksum.
- 2. Save the archive and checksum to your local machine.
- 3. Select the archive and checksum files in the upload form below.
- 4. Click Upload and Install to begin the update process.



- 4. Select the Archive and Checksum files.
- 5. Click Upload and Install.
- 6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

# 9.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

Protocol	Port	Purpose
TCP	22	SSH
TCP & UDP	53	DNS
TCP & UDP	123	NTP
TCP & UDP	161	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9080	WebUI - HTTP (disabled by default)
TCP	9081	Nginx fallback page
TCP	9443	WebUI - HTTPS

#### 9.6. HA Clustered Pair Configuration

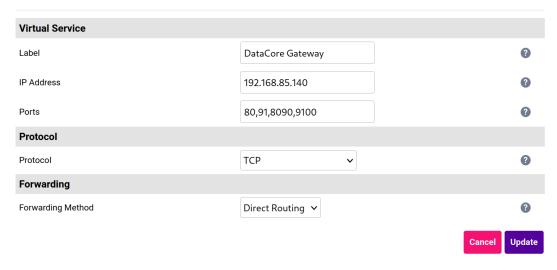
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in the section Configuring HA - Adding a Secondary Appliance of the appendix.

# 10. Appliance Configuration for DataCore Swarm GatewayUsing Layer 4 DR Mode

#### 10.1. Configuring the Virtual Service (VIP)

- 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. DataCore Gateway.
- 3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.140.
- 4. Set the *Ports* field to **80,91,8090,9100**.
- 5. Set the *Protocol* to **TCP**.
- 6. Leave the Forwarding Method set to Direct Routing.
- 7. Click **Update** to create the virtual service.

Layer 4 - Add a new Virtual Service

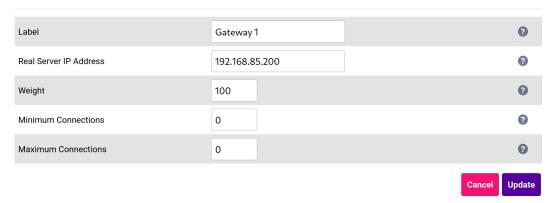


# 10.2. Defining the Real Servers (RIPs)

- 1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
- 2. Define the *Label* for the real server as required, e.g. **Gateway 1**.
- 3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.200.
- 4. Click Update.
- 5. Repeat these steps to add additional DateCore Swarm Gateways as real servers as required.



Layer 4 Add a new Real Server - DataCore\_Gateway



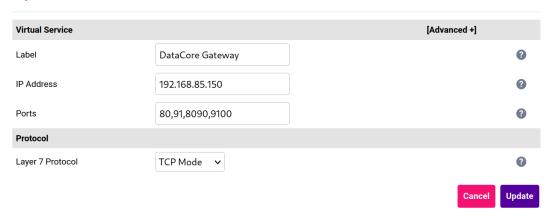
# 11. Appliance Configuration for DataCore Swarm Gateway

# Using Layer 7 SNAT Mode

# 11.1. Configuring the Virtual Service (VIP)

- 1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 Virtual Services* and click on **Add** a new Virtual Service.
- 2. Define the *Label* for the virtual service as required, e.g. **DataCore Gateway**.
- 3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.150.
- 4. Set the Ports field to 80,91,8090,9100.
- 5. Set the Layer 7 Protocol to TCP Mode.
- 6. Click **Update** to create the virtual service.

Layer 7 - Add a new Virtual Service

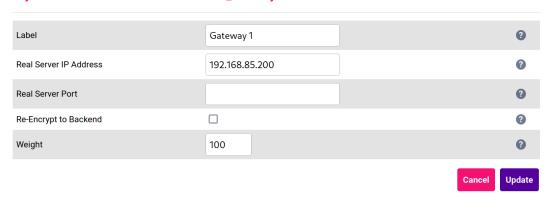


# 11.2. Defining the Real Servers (RIPs)

- 1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
- 2. Define the *Label* for the real server as required, e.g. **Gateway 1**.
- 3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.200.

- 4. Click Update.
- 5. Repeat these steps to add the remaining DataCore Swarm Gateways.

Layer 7 Add a new Real Server - DataCore\_Gateway



### 11.3. Finalizing the Layer 7 Configuration

To apply the new settings, HAProxy must be reloaded. This can be done using the button in the "Commit changes" box at the top of the screen or by using the *Restart Services* menu option:

- 1. Using the WebUI, navigate to: Maintenance > Restart Services.
- 2. Click Reload HAProxy.

# 12. Testing & Verification

8 Note

For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

# 12.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the DataCore Swarm Gateway servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows a standard deployment where both DataCore Swarm Gateway servers are healthy and available to accept connections:

#### 2023-07-20 16:19:03 UTC VIRTUAL SERVICE **♦** IP **♦** PORTS **♦** CONNS **♦** PROTOCOL **♦** METHOD **♦** MODE **♦** DataCore\_Gateway.. 192.168.85.140 80,91,809.. **TCP** Layer 4 DR REAL SERVER **PORTS** WEIGHT CONNS 0 Gateway 1 192.168.85.200 80,91,8090.. 100 Drain Halt Gateway 2 80,91,8090.. 100 0 Drain 192.168.85.201 Halt

# 13. 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: <a href="support@loadbalancer.org">support@loadbalancer.org</a>.

# 14. Further Documentation

For additional information, please refer to the Administration Manual.



# 15. Appendix

#### 15.1. 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 is configured first and 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.

8 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.

#### Non-Replicated Settings

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:

WebUl Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	All network settings including IP address(es), bonding configuration and VLANs
Local Configuration	Routing	Routing configuration including default gateways and static routes
Local Configuration	System Date & time	All time and date related settings
Local Configuration	Physical – Advanced Configuration	Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server
Local Configuration	Security	Appliance security settings
Local Configuration	SNMP Configuration	Appliance SNMP settings
Local Configuration	Graphing	Appliance graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Software Updates	Appliance software update management
Maintenance	Firewall Script	Appliance firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

(!) Important

Make sure that if these settings/updates have been configured on the Primary appliance, they're also configured on the Secondary appliance.

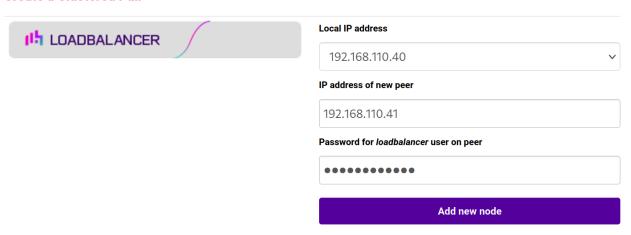
#### Adding a Secondary Appliance - Create an HA Clustered Pair

8 Note

If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

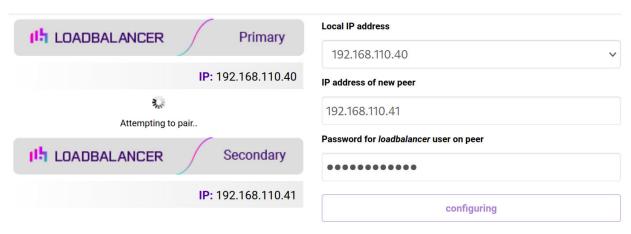
- 1. Deploy a second appliance that will be the Secondary and configure initial network settings.
- 2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.

#### **Create a Clustered Pair**



- 3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown in the example above.
- 4. Click Add new node.
- 5. The pairing process now commences as shown below:

#### **Create a Clustered Pair**



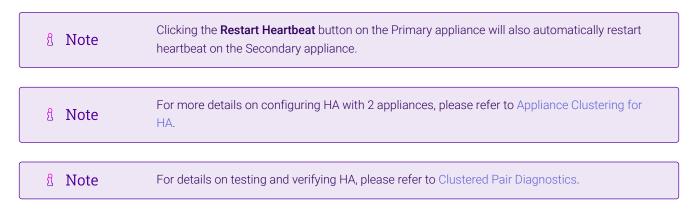
6. Once complete, the following will be displayed on the Primary appliance:



#### **High Availability Configuration - primary**



7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.



# 16. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	20 July 2023	Initial version		АН





Visit us: www.loadbalancer.org

**Phone us:** +44 (0)330 380 1064

**Phone us:** +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: @loadbalancer.org

#### **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.

