LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Storage Made Easy File Fabric

Version 1.2.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced Storage Made Easy File Fabric environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any File Fabric configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing File Fabric. For full specifications of available models please refer to https://www.loadbalancer.org/products/enterprise.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

> **Note** The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. File Fabric

- Version 1906.00 and later

4. Storage Made Easy File Fabric

Storage Made Easy provides an on-premises Enterprise File Fabric solution which is storage agnostic and can be used either with a single storage back-end or multiple public/private storage systems. In the event of the latter, the File Fabric unifies the view across all access clients and implements a common control and governance policies through the use of its cloud control features.

The product is supplied as a software 'appliance' which is run inside of a hypervisor and consists of a pre-configured, 'hardened' operating system (CentOS) and the File Fabric Application provided by Storage Made Easy.

5. Load Balancing File Fabric

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

5.1. Load Balancing & HA Requirements

To deploy File Fabric as an HA deployment, 4 SME File Fabric instances are needed. When configured as per the Storage Made Easy guides, the topology will be as follows:

- 2 SME Web servers
- 2 SME SQL servers

5.2. Persistence (aka Server Affinity)

Load balancing File Fabric requires source IP address affinity. This is true for both the layer 4 and layer 7 based load balancing methods described in this document.

5.3. Virtual Service (VIP) Requirements

To provide load balancing and HA for File Fabric, the following VIPs are required:

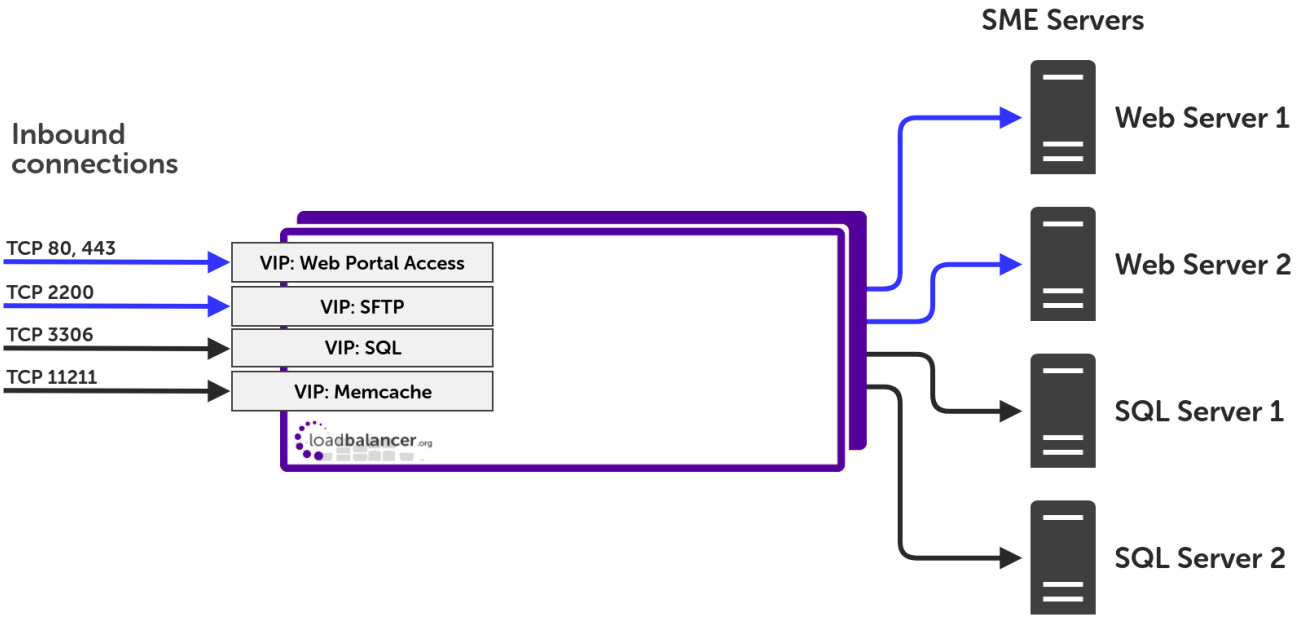
- Web portal access
- SQL
- Memcache
- SFTP

5.4. Port Requirements

The following table shows the ports that are load balanced:

Port	Protocols	Use
80	TCP/HTTP	Web Portal Access over HTTP
443	TCP/HTTPS	Web Portal Access over HTTPS
3306	TCP/SQL	SQL Service
2200	TCP/SFTP	SFTP Service
11211	TCP/Memcache	Memcache Service

6. Deployment Concept



VIP = **V**irtual **IP** Address

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

7. Load Balancer Deployment Methods

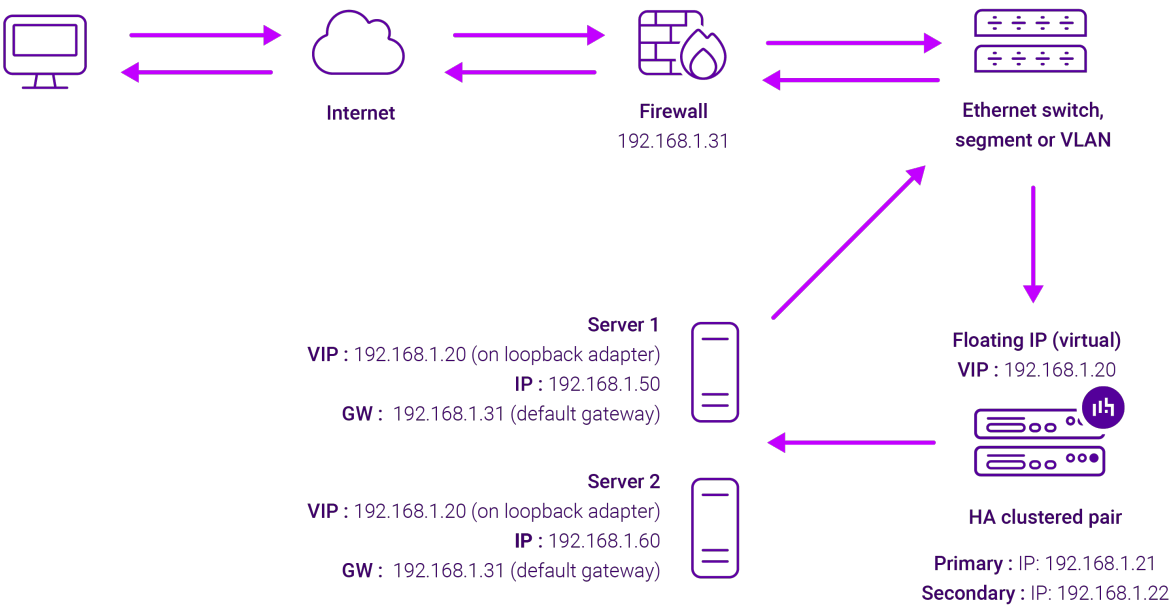
The load balancer can be deployed in 4 fundamental ways: ***Layer 4 DR mode***, ***Layer 4 NAT mode***, ***Layer 4 SNAT mode,*** and ***Layer 7 SNAT mode***.

For File Fabric, using a combination of layer 4 DR mode and layer 7 SNAT mode is recommended. It it also possible to only use layer 7 SNAT mode, however the performance of this set up is not as great and client source IP addresses are not passed through to the SME servers on the back end. Both of these setups are described below and are used for the configurations presented in this guide. For configuring using a combination of layer 4 DR mode and layer 7 SNAT mode please refer to Appliance Configuration for File Fabric – Using Layer 4 DR Mode and Layer 7 SNAT Mode. For configuring using only layer 7 SNAT mode refer to Appliance Configuration for File Fabric – Using Only Layer 7 SNAT Mode.

7.1. Layer 4 DR Mode

Layer 4 DR (Direct Routing) mode is a very high performance solution that requires little change to your existing infrastructure. The image below shows an example network diagram for this mode.

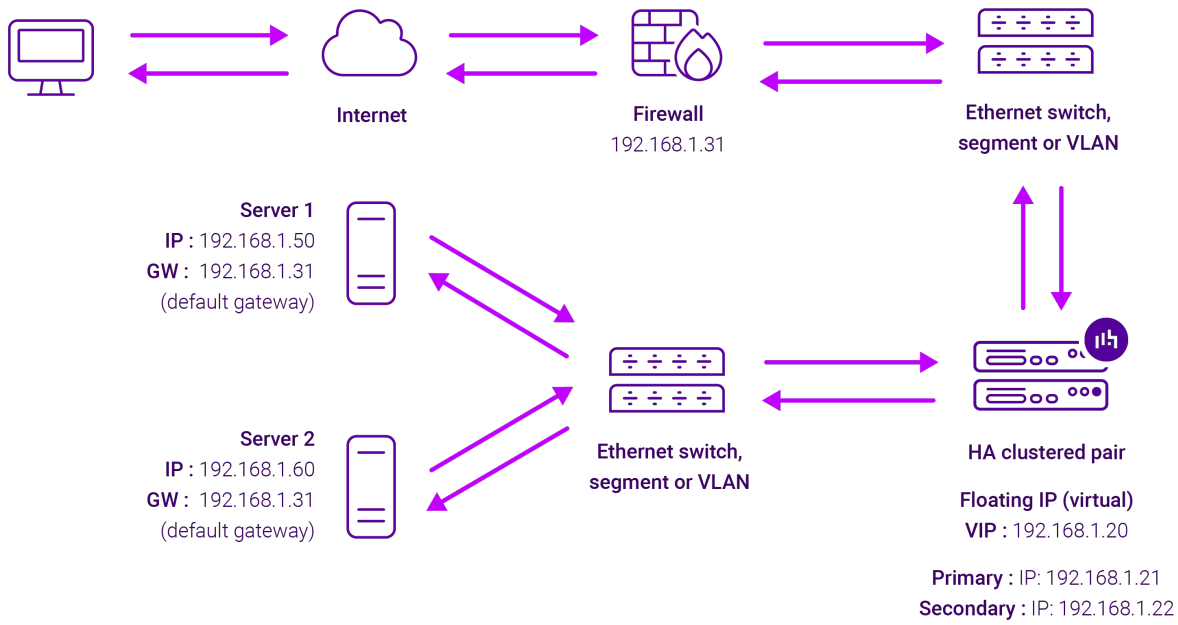
> **Note** Kemp, Brocade, Barracuda & A10 Networks call this ***Direct Server Return*** and F5 call it ***nPath***.



- 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 each Real Server (and the load balanced application) must respond to both the Real Server's own IP address and the VIP.
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Server 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 mode for HTTP and much faster for other applications such as Remote Desktop Services, streaming media and FTP.
- The load balancer must have an interface in the same subnet as the Real Servers to ensure layer 2 connectivity which is required for DR mode to operate.
- 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. The image below shows an example network diagram for this mode.



- Because layer 7 SNAT mode is a full proxy, Real Servers in the cluster can be on any accessible network 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, **eth1** is typically used for client side connections and **eth0** is used for Real Server connections, although this is not mandatory since any interface can be used for any purpose.
- 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

Where possible, we recommend that the combination of Layer 4 Direct Routing (DR) mode and Layer 7 SNAT mode is used. This mode offers the best possible performance for the DR mode services, since replies go directly from the Real Servers to the client and not via the load balancer. It's also relatively simple to implement. Ultimately, the final choice does depend on your specific requirements and infrastructure.

If DR mode cannot be used, for example if the real servers are located in remote routed networks, then SNAT mode is recommended. SNAT mode is also recommended if it is not possible to make network adaptor changes to the SME servers, for example if you do not own or do not control the infrastructure.

If the load balancer is deployed in AWS, Azure, or GCP, layer 7 SNAT mode must be used as layer 4 direct routing is not currently possible on these platforms.

8. Configuring File Fabric for Load Balancing

Ensure that a working, HA File Fabric deployment is in place prior to deploying a load balancer.

Refer to the following Storage Made Easy documentation for guidance on how to achieve this:

Installation: Getting Started: File Fabric On-Premises

File Fabric HA Master - Master Database with Automatic Failover

SME How to configure SFTP

When using the load balancer setup that makes use of layer 4 DR mode, the ARP problem must be solved on each SME server. Please refer to Solving the ARP Problem for instructions on how to do this.

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.

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 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.

Note	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 servers and other network and administrative settings.

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.

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

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

   > **Note** You'll receive a warning about the WebUI's SSL 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.

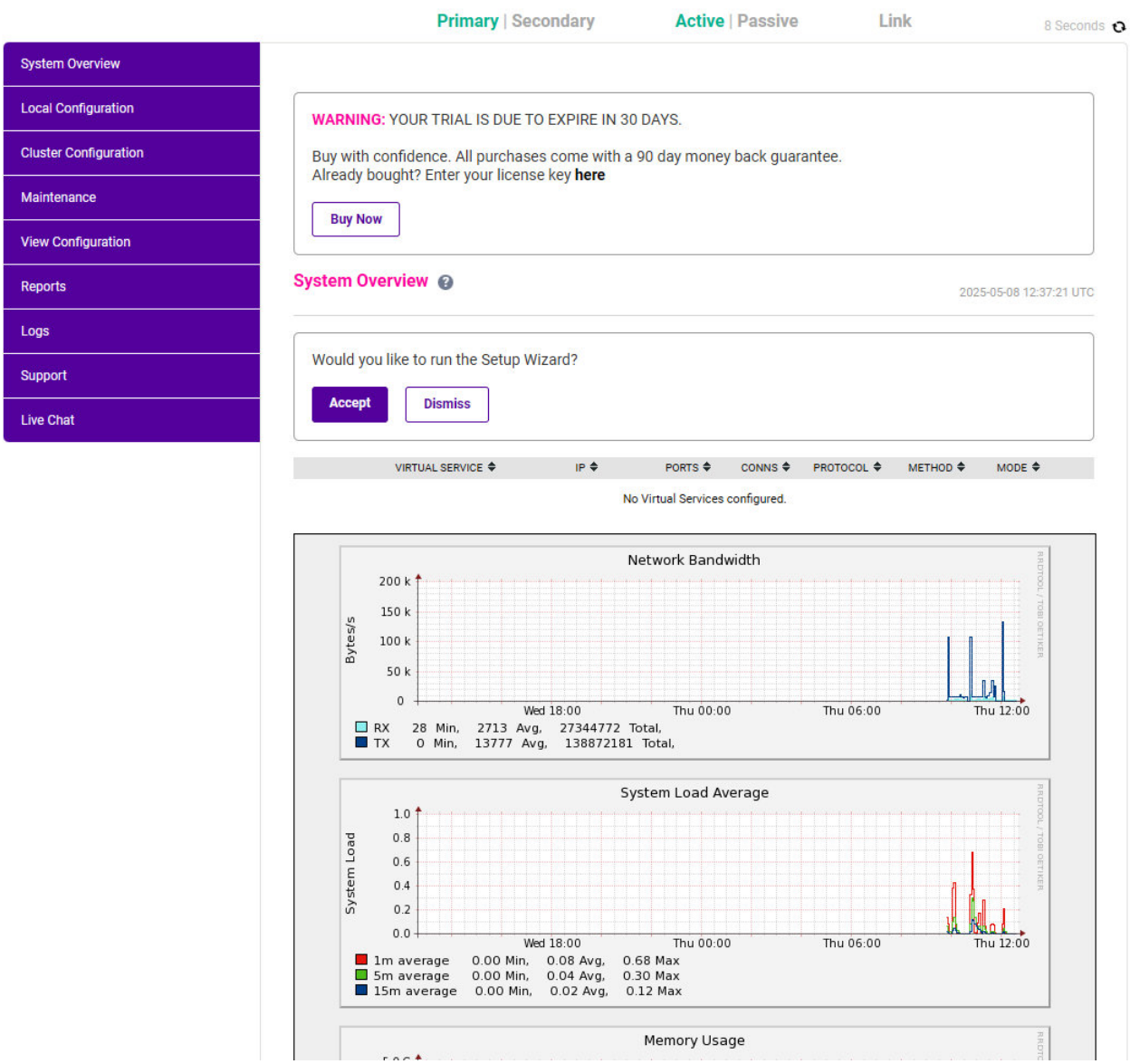
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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:



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.

9.3.1. 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 creating backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links

Live Chat - Start a live chat session with one of our Support Engineers

9.4. Appliance Software Update

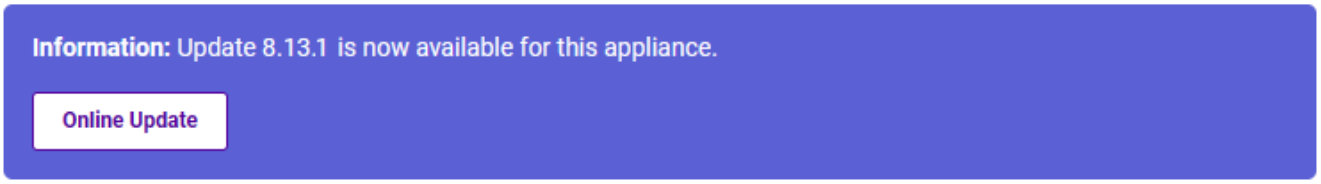
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **Note** For full details, please refer to Appliance Software Update in the Administration Manual.

> **Note** Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

9.4.1. Online Update

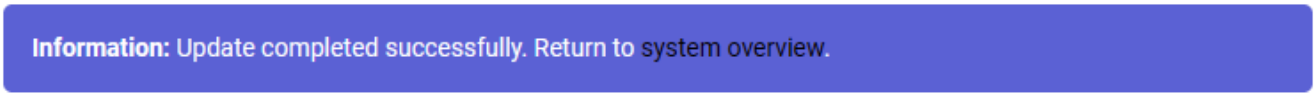
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

> **Important** Do not navigate away whilst the update is ongoing, this may cause the update to fail.

The update can take several minutes depending on download speed and upgrade version. Once complete, the following message will be displayed:



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

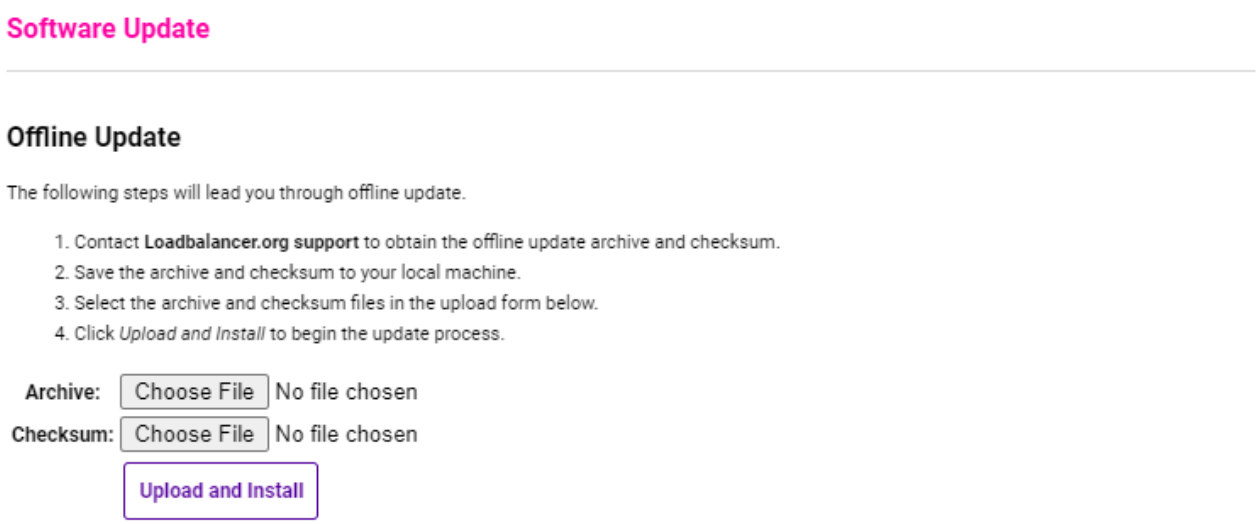
9.4.2. Offline Update

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

To check for the latest version, please refer to our product roadmap page available here. To obtain the latest offline update files contact support@loadbalancer.org.

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:



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 / GSLB
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	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page
TCP	9443 *	WebUI - HTTPS
TCP	25565 *	Shuttle service (Centralized/Portal Management)

> **Note** The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket

Addresses.

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 Configuring HA - Adding a Secondary Appliance.

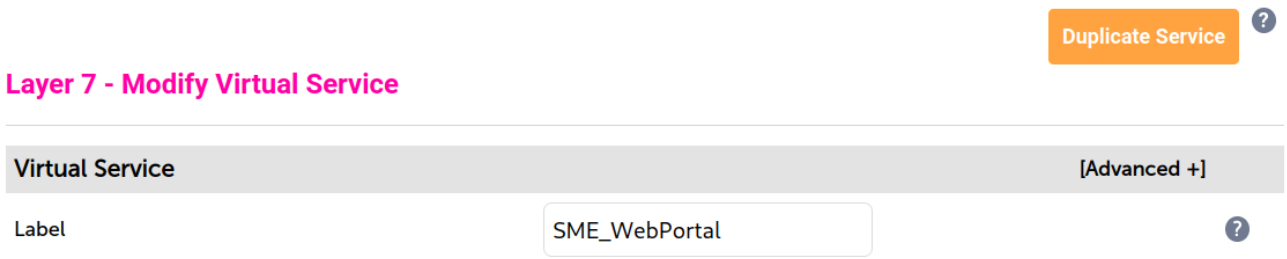
10. Appliance Configuration for File Fabric – Using Layer 4 DR Mode and Layer 7 SNAT Mode

10.1. Duplicate Service Function

As of version 8.3.8 of the Loadbalancer.org appliance, the **Duplicate Service** button can be used to save time during initial configuration. This function duplicates the configuration of a given virtual service along with all of the associated back end real servers which have been defined. This is useful for deployments where multiple, very similar virtual services are used, with only minor changes between them. It saves time as the same settings and real servers do not need to be repeatedly defined.

First, fully create the initial virtual service as directed. Then click the *Modify* button for the virtual service in question, click the **Duplicate Service** button near the top, and make the necessary changes for the new, duplicated virtual service.

This feature is available for both layer 4 and layer 7 virtual services.



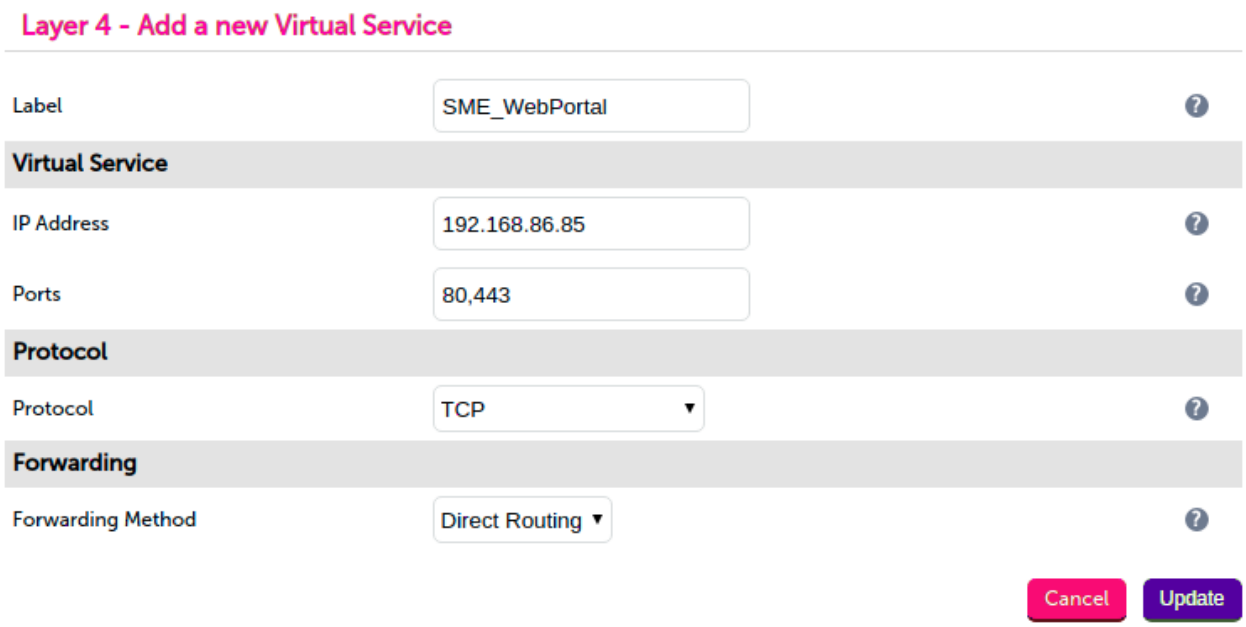
10.2. Layer 4 Direct Routing Configuration

10.2.1. Configuring VIP 1 – SME Web Portal

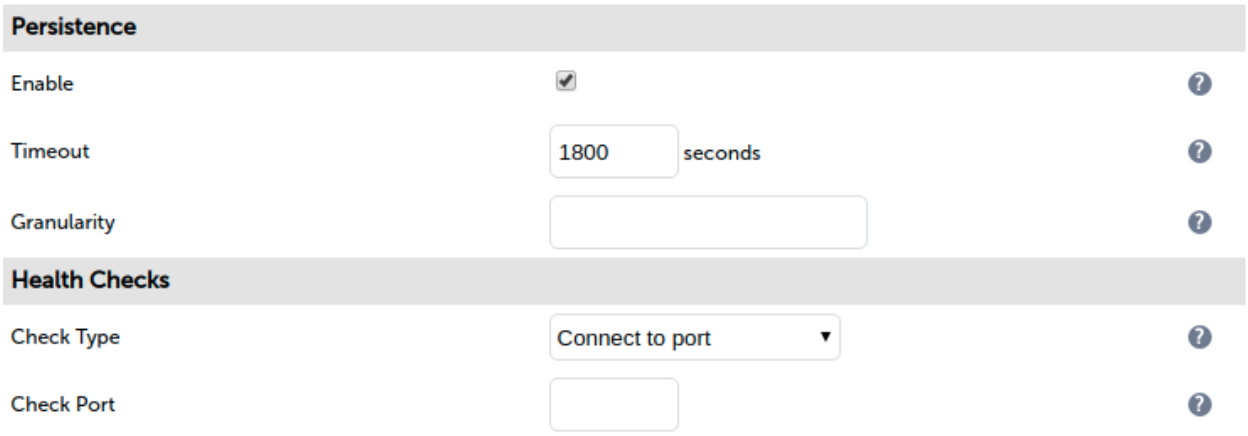
Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **SME_WebPortal**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.86.84**.
4. Set the *Ports* field to **80,443**.
5. Leave the *Protocol* set to **TCP**.

6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the virtual service.



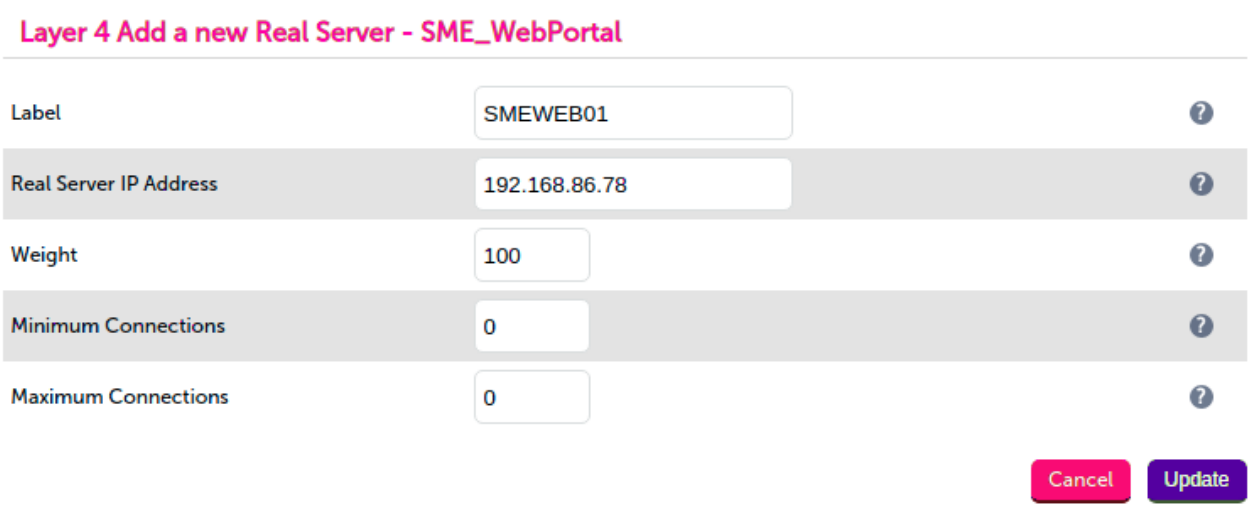
8. Click **Modify** next to the newly created VIP.
9. Ensure that the *Persistence Enable* checkbox is checked and that the *Timeout* is set to **1800**.
10. Leave the *Health Checks Check Type* set to **Connect to port**.
11. Click **Update**.



Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **SMEWEB01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.86.78**.
4. Click **Update**.

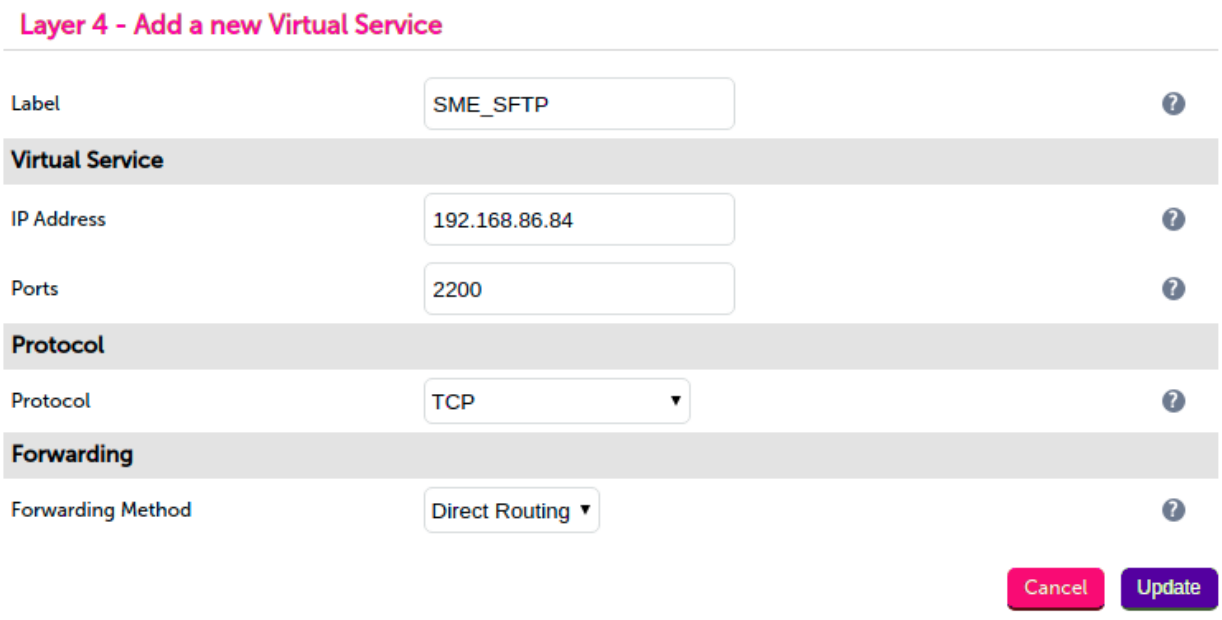
5. Repeat these steps to add additional SME servers as required.



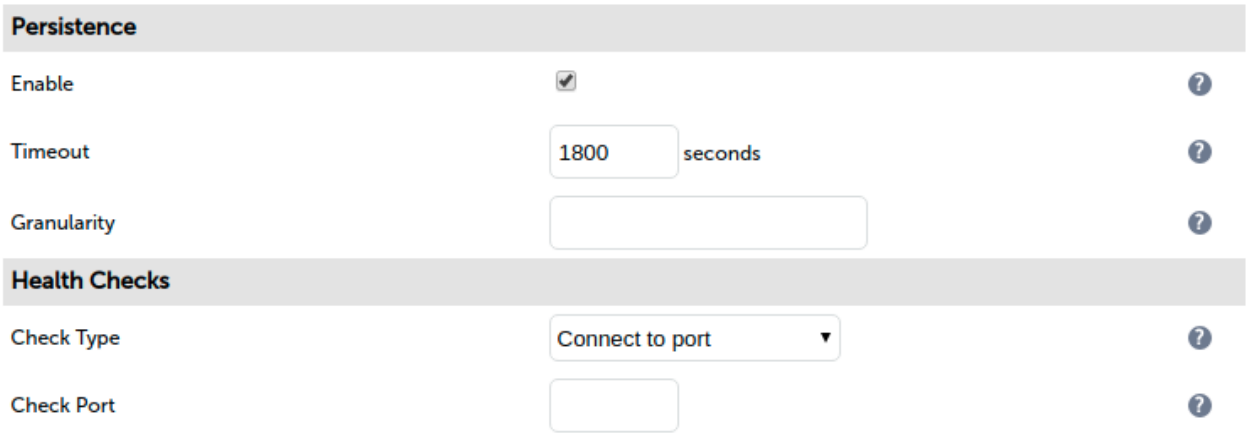
10.2.2. Configuring VIP 2 – SME SFTP

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **SME_SFTP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.86.84**.
4. Set the *Ports* field to **2200**.
5. Leave the *Protocol* set to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the virtual service.

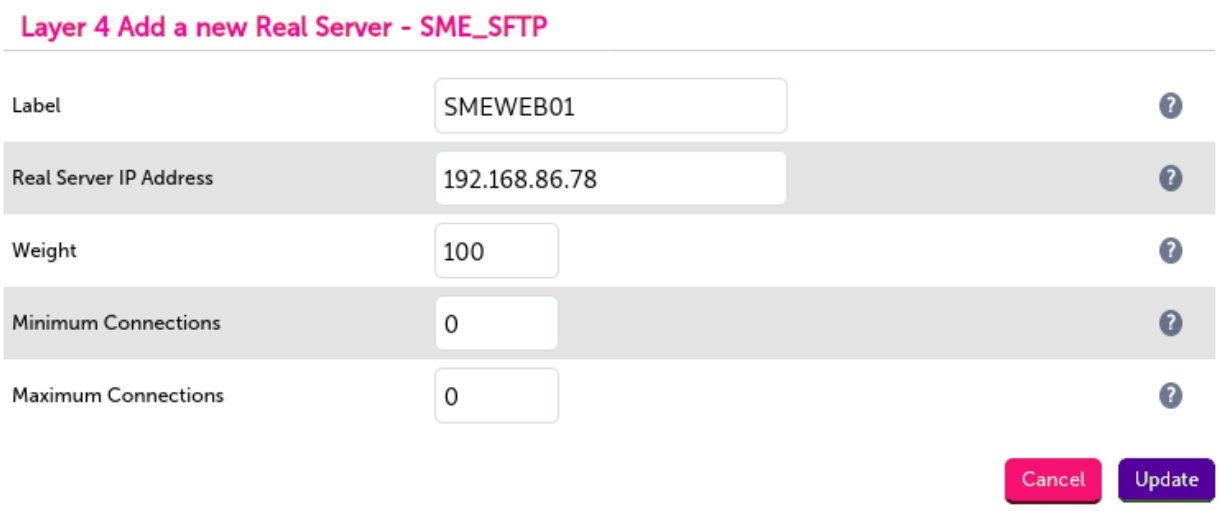


8. Click **Modify** next to the newly created VIP.
9. Ensure that the *Persistence Enable* checkbox is checked and that the *Timeout* is set to **1800**.
10. Leave the *Health Checks Check Type* set to **Connect to port**.
11. Click **Update**.



Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **SMEWEB01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.86.78**.
4. Click **Update**.
5. Repeat these steps to add additional SME servers as required.



10.3. Layer 7 SNAT Mode Configuration

To load balance the SQL and Memcache services, layer 7 virtual services should be used. This is because layer 4 direct routing mode does not provide any real benefit or advantage for these services.

To set up layer 7 virtual services for SQL and Memcache, follow the appropriate instructions from the next section of this document, *Appliance Configuration for File Fabric – Using Only Layer 7 SNAT Mode*, i.e.:

- Configuring VIP 3 – SME SQL
- Configuring VIP 4 – SME Memcache
- Finalizing the Configuration

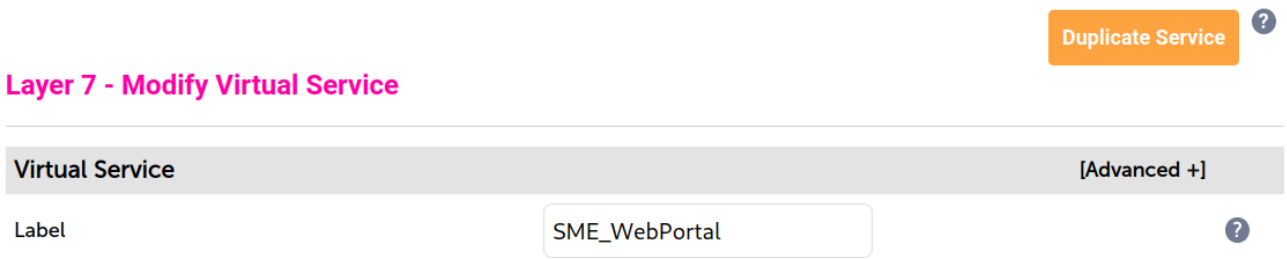
11. Appliance Configuration for File Fabric – Using Only Layer 7 SNAT Mode

11.1. Duplicate Service Function

As of version 8.3.8 of the Loadbalancer.org appliance, the **Duplicate Service** button can be used to save time during initial configuration. This function duplicates the configuration of a given virtual service along with all of the associated back end real servers which have been defined. This is useful for deployments where multiple, very similar virtual services are used, with only minor changes between them. It saves time as the same settings and real servers do not need to be repeatedly defined.

First, fully create the initial virtual service as directed. Then click the *Modify* button for the virtual service in question, click the **Duplicate Service** button near the top, and make the necessary changes for the new, duplicated virtual service.

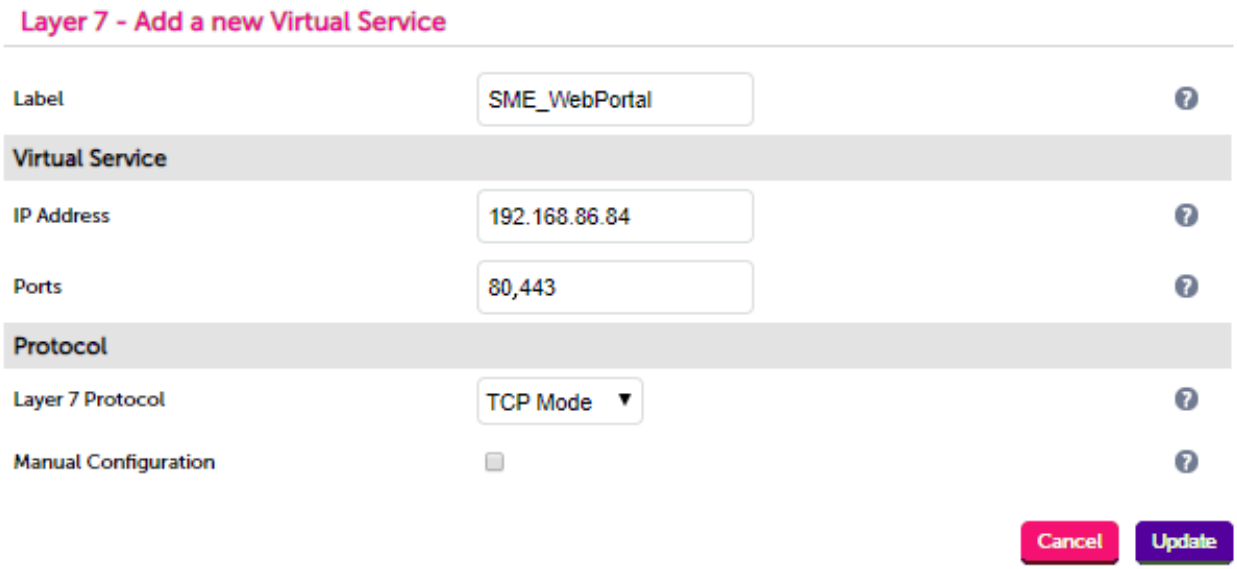
This feature is available for both layer 4 and layer 7 virtual services.



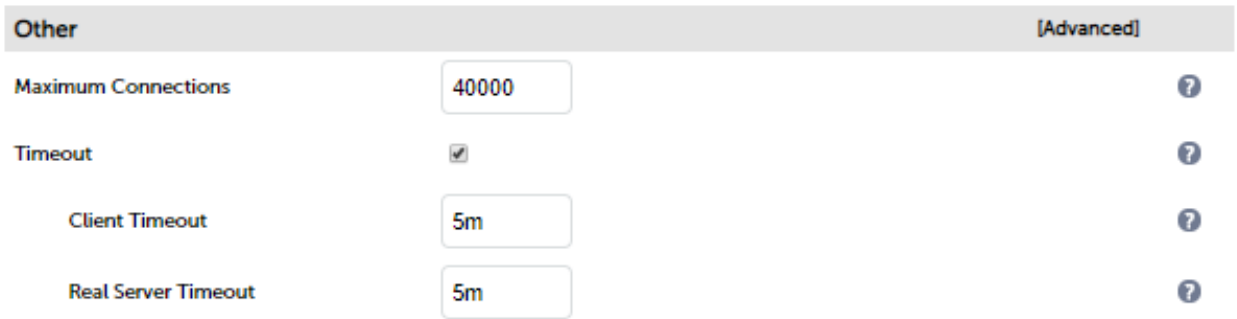
11.2. Configuring VIP 1 – SME Web Portal

11.2.1. 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. **SME_WebPortal**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.86.84**.
4. Set the *Virtual Service Ports* field to **80,443**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.



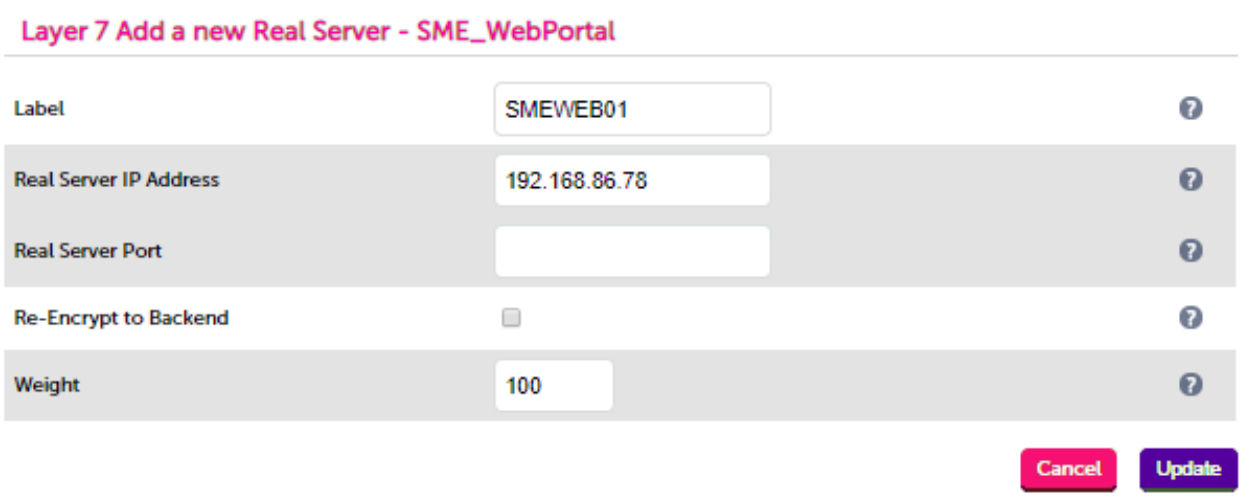
7. Click **Modify** next to the newly created VIP.
8. Set *Persistence Mode* to **Source IP**.
9. Set *Health Checks* to **Connect to port**.
10. In the *Other* section click **Advanced** to expand the menu.
11. Check the **Timeout** checkbox.
12. Set *Client Timeout* to **5m** (this is 5 minutes).
13. Set *Real Server Timeout* to **5m**.
14. Click **Update**.



11.3. 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. Enter an appropriate name for the server in the *Label* field, e.g. **SMEWEB01**.
3. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.86.78**.
4. Click **Update**.

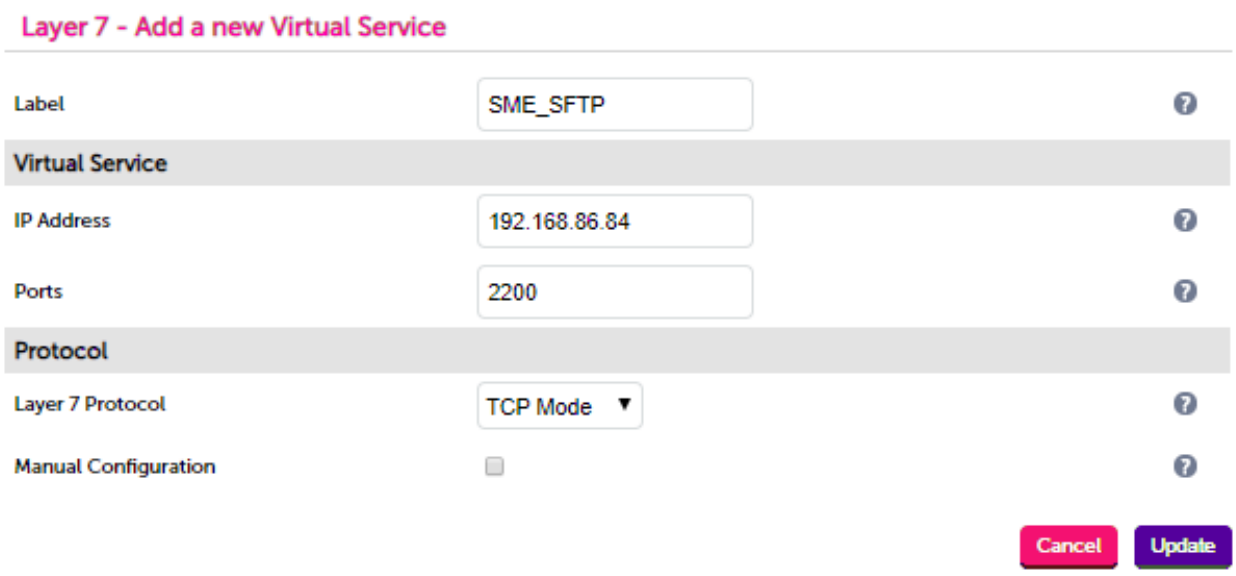
5. Repeat these steps to add additional servers as required.



11.4. Configuring VIP 2 – SME SFTP

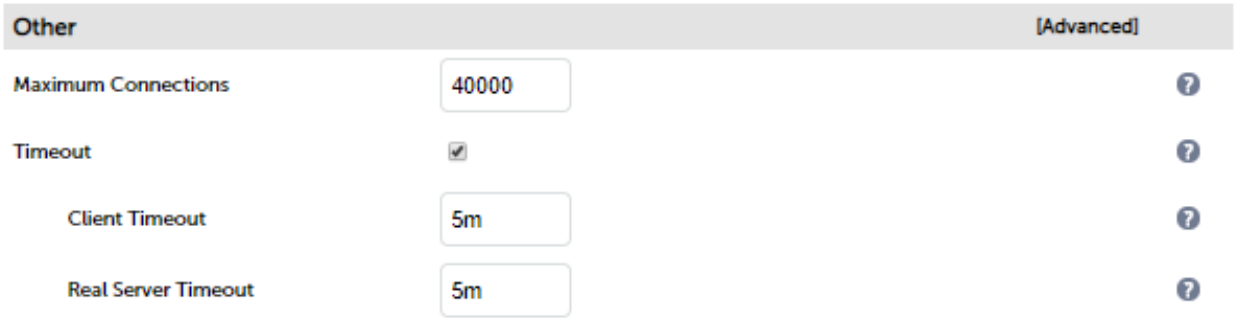
11.4.1. Configuring the Virtual Service (VIP)

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. **SME_SFTP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.86.84**.
4. Set the *Virtual Service Ports* field to **2200**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.



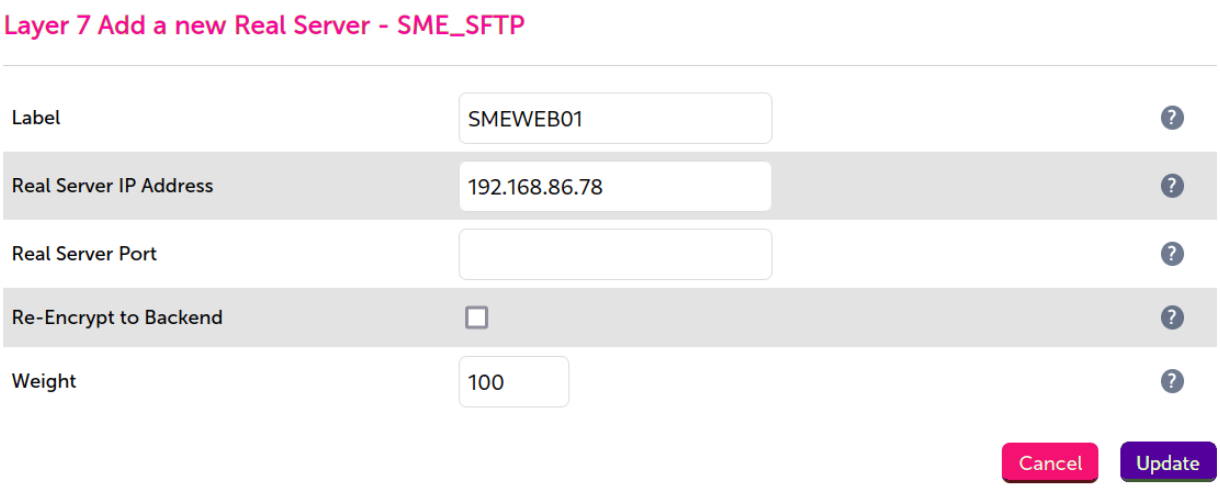
7. Click **Modify** next to the newly created VIP.
8. Set *Persistence Mode* to **Source IP**.

9. Set *Health Checks* to **Connect to port**.
10. In the *Other* section click **Advanced** to expand the menu.
11. Check the **Timeout** checkbox.
12. Set *Client Timeout* to **5m** (this is 5 minutes).
13. Set *Real Server Timeout* to **5m**.
14. Click **Update**.



11.5. 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. Enter an appropriate name for the server in the *Label* field, e.g. **SMEWEB01**.
3. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.86.78**.
4. Click **Update**.
5. Repeat these steps to add additional servers as required.

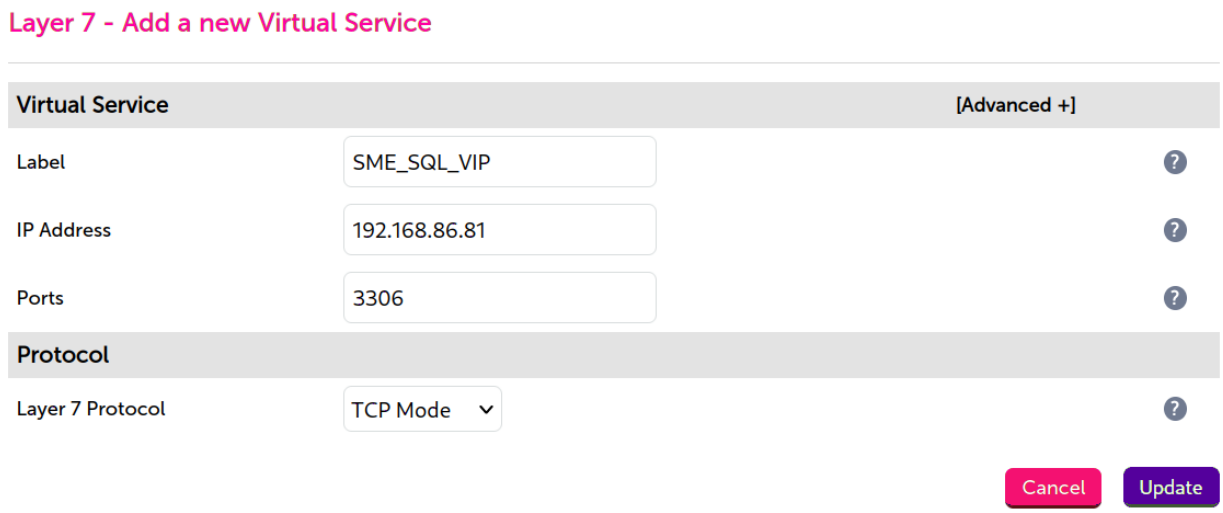


11.6. Configuring VIP 3 – SME SQL

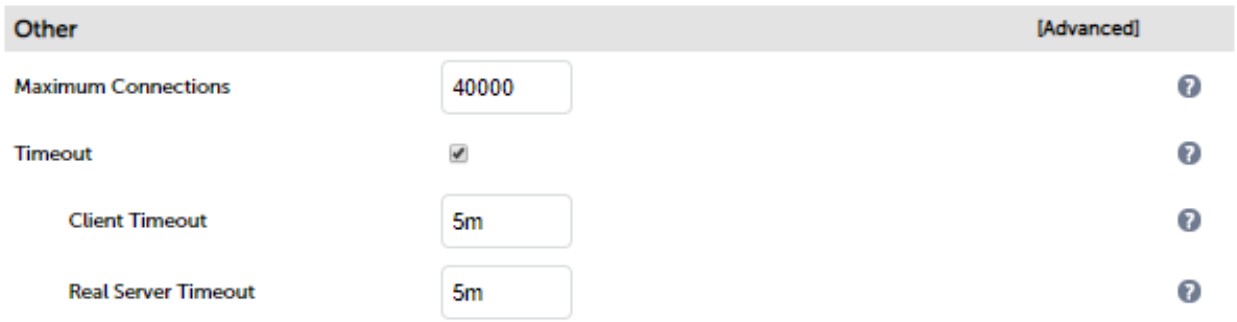
11.6.1. Configuring the Virtual Service (VIP)

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. **SME_SQL_VIP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.86.81**.
4. Set the *Virtual Service Ports* field to **3306**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.



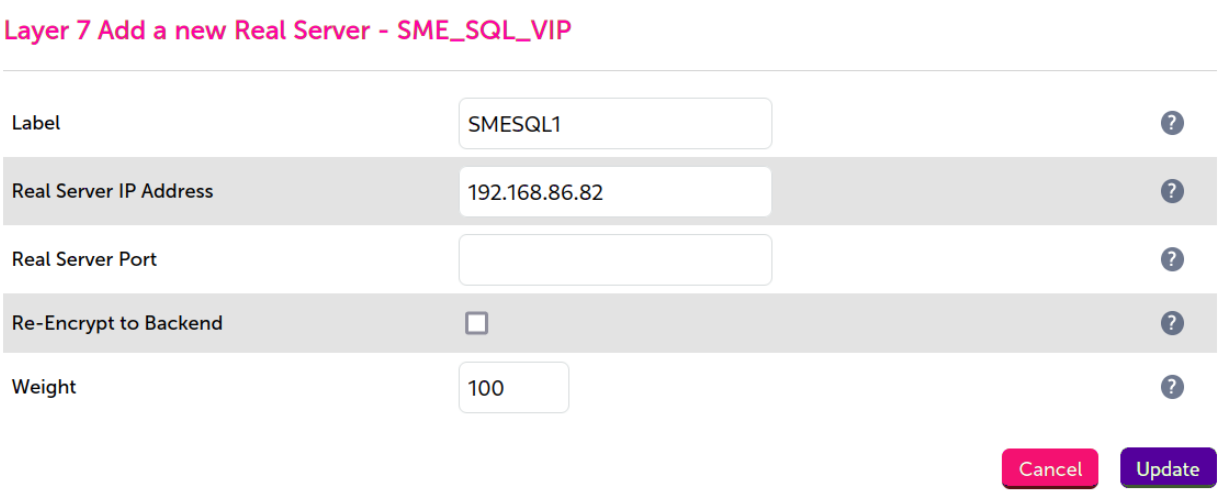
7. Click **Modify** next to the newly created VIP.
8. Set *Persistence Mode* to **Source IP**.
9. Set *Health Checks* to **Connect to port**.
10. In the *Other* section click **Advanced** to expand the menu.
11. Check the **Timeout** checkbox.
12. Set *Client Timeout* to **5m** (this is 5 minutes).
13. Set *Real Server Timeout* to **5m**.
14. Click **Update**.



11.7. 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.

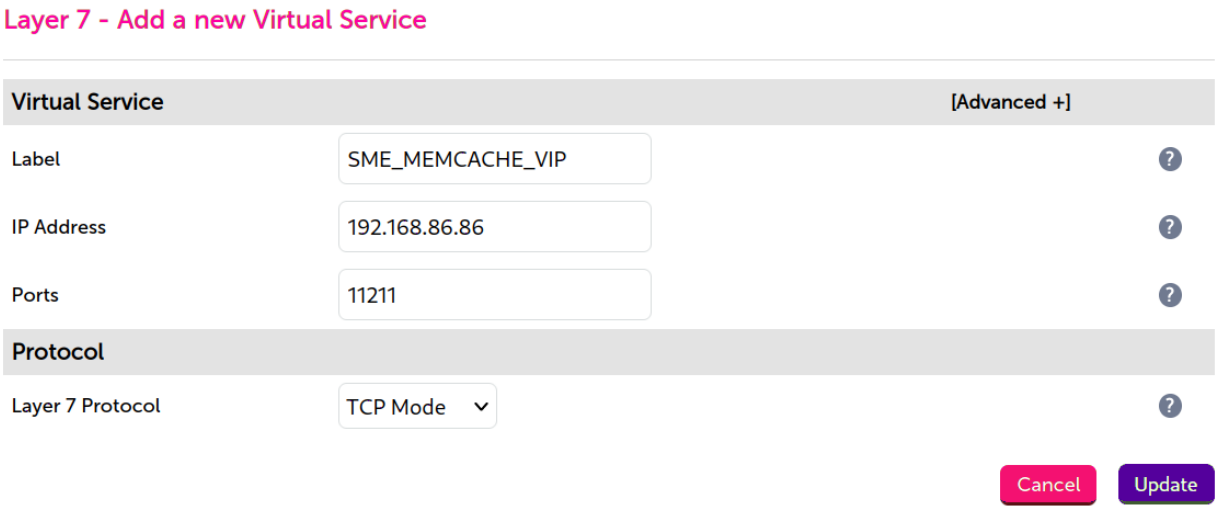
2. Enter an appropriate name for the server in the *Label* field, e.g. **SMESQL01**.
3. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.86.82**.
4. Click **Update**.
5. Repeat these steps to add additional servers as required.



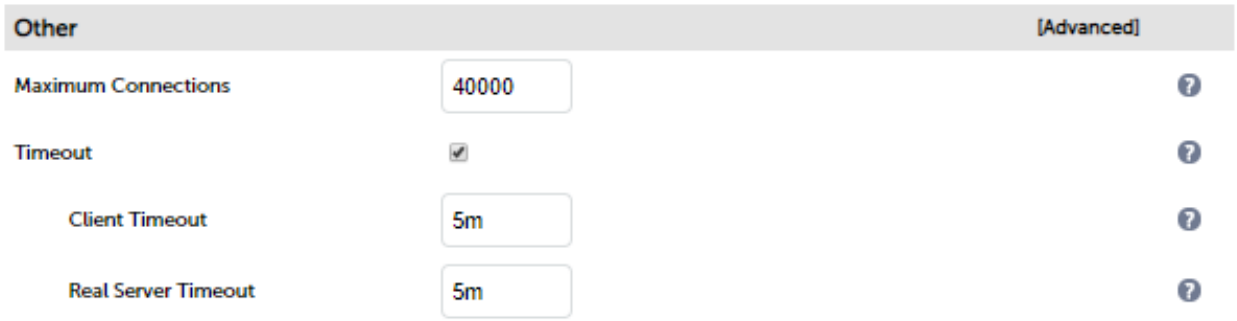
11.8. Configuring VIP 4 – SME Memcache

11.8.1. 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. **SME_MEMCACHE_VIP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.86.86**.
4. Set the *Virtual Service Ports* field to **11211**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.

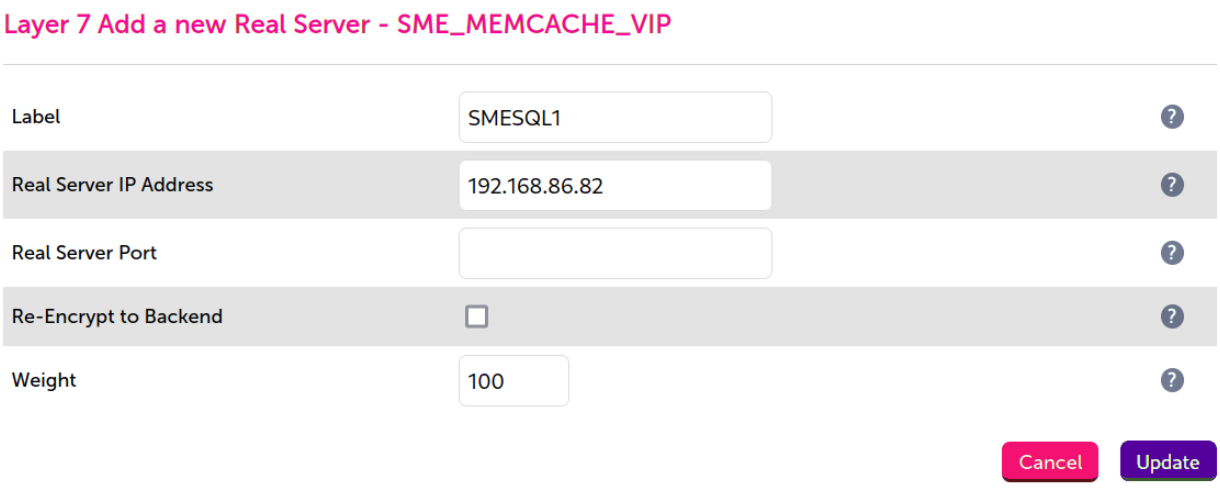


7. Click **Modify** next to the newly created VIP.
8. Set *Persistence Mode* to **Source IP**.
9. Set *Health Checks* to **Connect to port**.
10. In the *Other* section click **Advanced** to expand the menu.
11. Check the **Timeout** checkbox.
12. Set *Client Timeout* to **5m** (this is 5 minutes).
13. Set *Real Server Timeout* to **5m**.
14. Click **Update**.



11.9. 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. Enter an appropriate name for the server in the *Label* field, e.g. **SMESQL01**.
3. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.86.82**.
4. Click **Update**.
5. Repeat these steps to add additional servers as required.



11.10. Finalizing the 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:

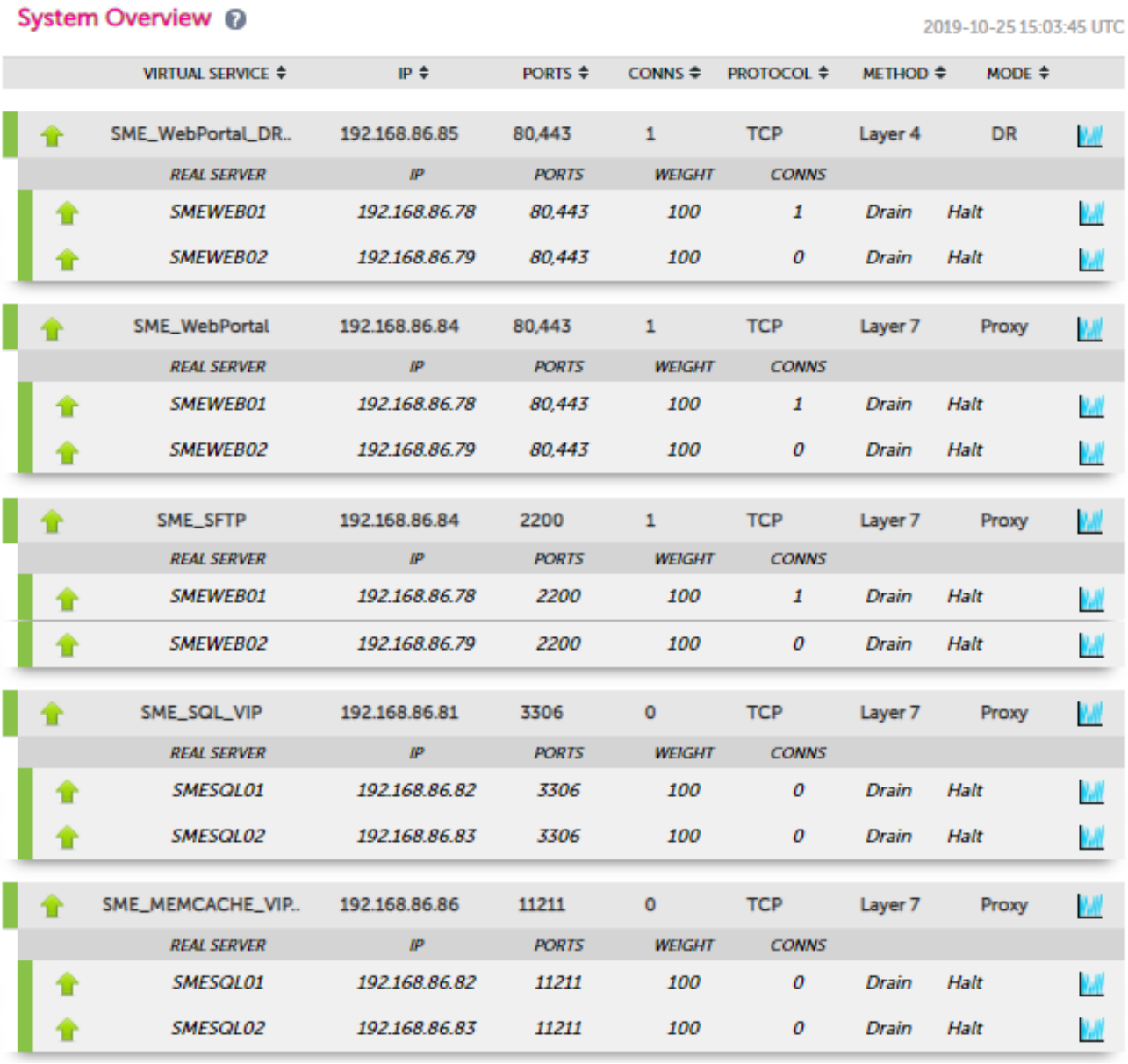
1. Using the WebUI, navigate to: *Maintenance > Restart Services*.
2. Click **Reload HAProxy**.

12. Testing & Verification

> **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 SME servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows that both SME servers are healthy, across all 5 virtual services, and available to accept connections:

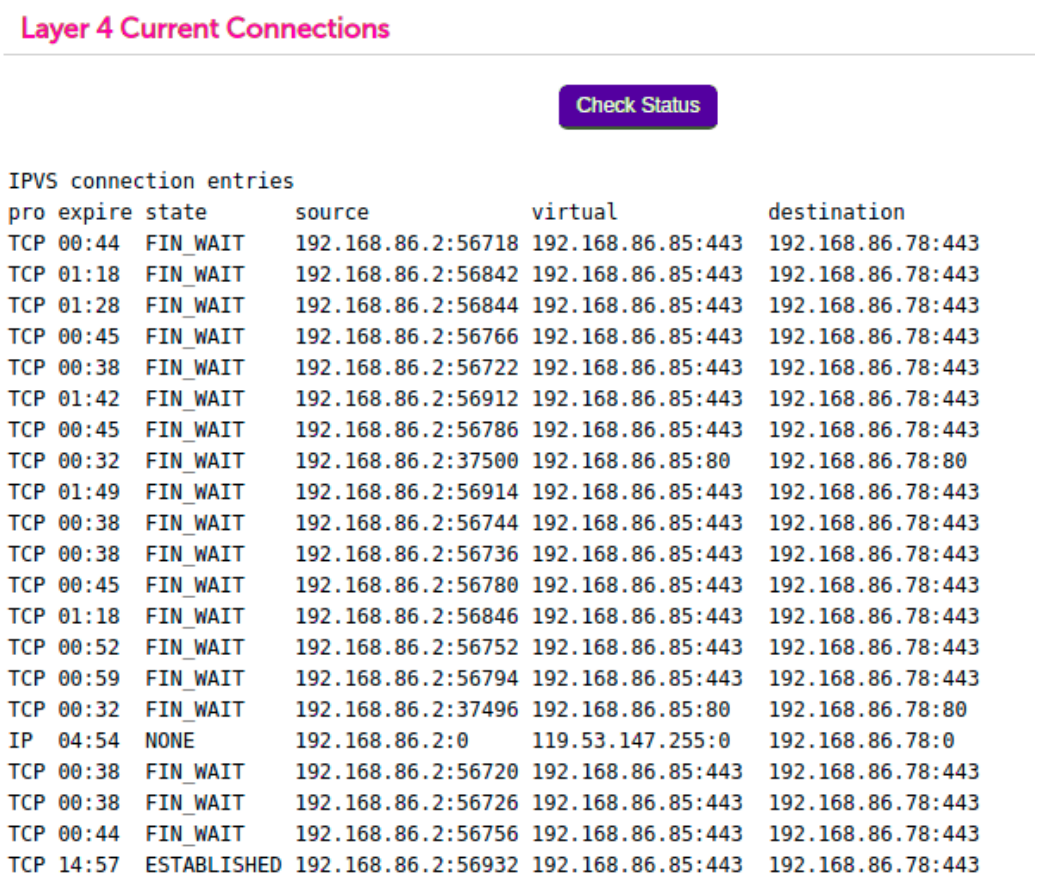


12.2. Layer 4 Direct Routing Specific Check

If using the setup that combines layer 4 DR mode and layer 7 SNAT mode, it is possible to specifically check that layer 4 DR mode has been correctly configured (including verifying that the real servers have been modified correctly in regards to the *ARP problem*).

After sending traffic to the layer 4 DR mode virtual services, check that connections are not in the **SYN_RECV** state and that they are **ESTABLISHED**. This can be done through the load balancer's WebUI, by navigating to *Reports > Layer 4 Current Connections*.

If there are a significant number of connections in the **SYN_RECV** state then that implies that the *ARP problem* has not been correctly resolved on the back end real servers.



12.3. SFTP Service Check

For details on how to perform a check of the SFTP service, see Testing the SFTP Service.

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: support@loadbalancer.org.

14. Further Documentation

For additional information, please refer to the Administration Manual.

15. Appendix

15.1. Solving the ARP Problem

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

15.1.1. Windows Server 2012 & Later

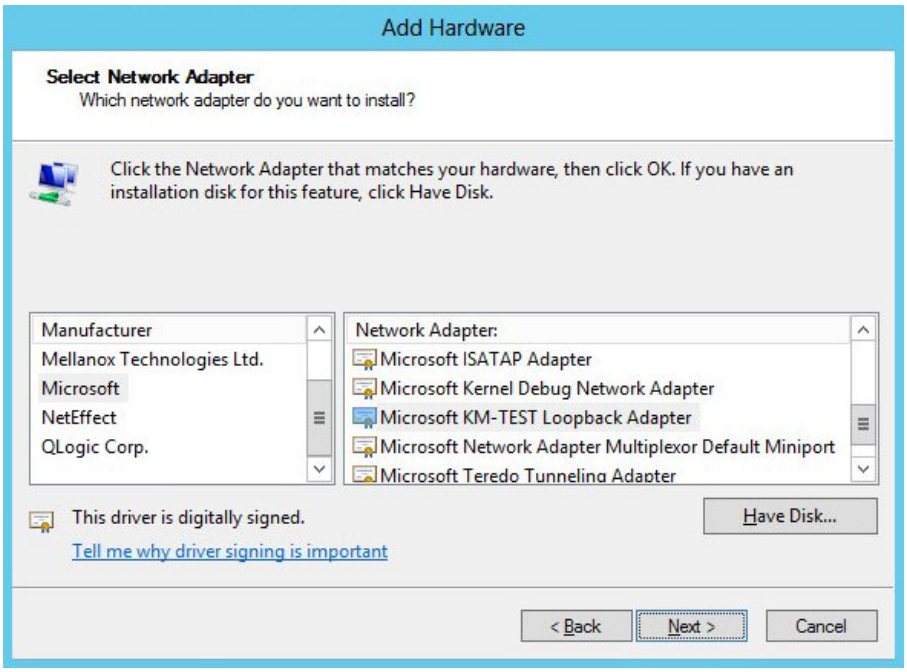
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables the server to receive packets that have their destination set as the VIP address. If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

In addition, the strong/weak host behavior must be configured on each Real Server. The weak host model allows packets with any IP to be sent or received via an interface. The strong host model only allows packets with an IP belonging to the interface to be sent or received.

> **Important** The following 3 steps must be completed on ***all*** Real Servers associated with the VIP.

Step 1 of 3: Install the Microsoft Loopback Adapter

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
2. Once 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**.

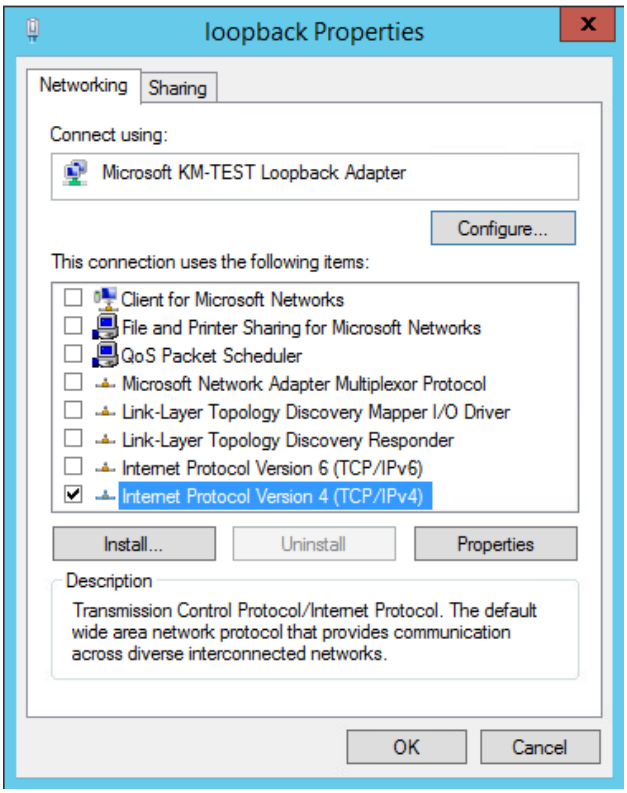
Step 2 of 3: Configure the Loopback Adapter

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**.

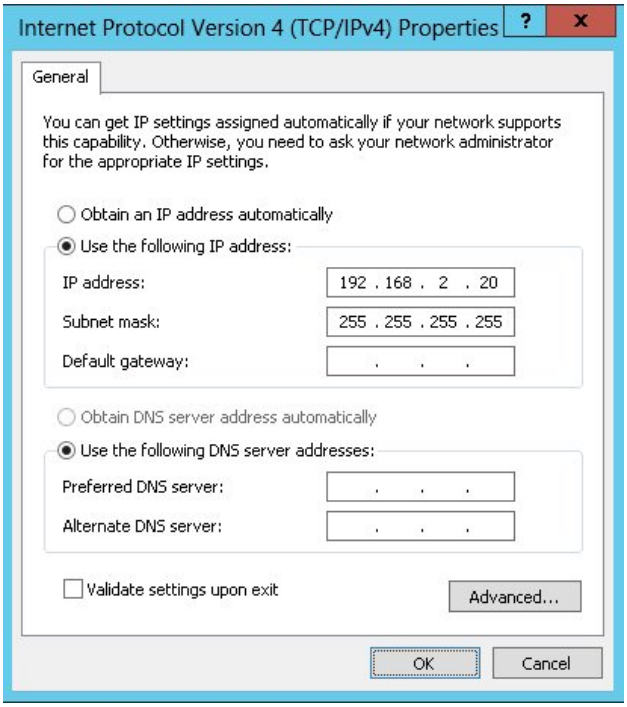
> **Note** You can configure IPv4 or IPv6 addresses or both depending on your requirements.

IPv4 Addresses

1. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below:



2. Ensure that **Internet Protocol Version (TCP/IPv4)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service address (VIP) with a subnet mask of **255.255.255.255**, e.g. **192.168.2.20/255.255.255.255** as shown below:



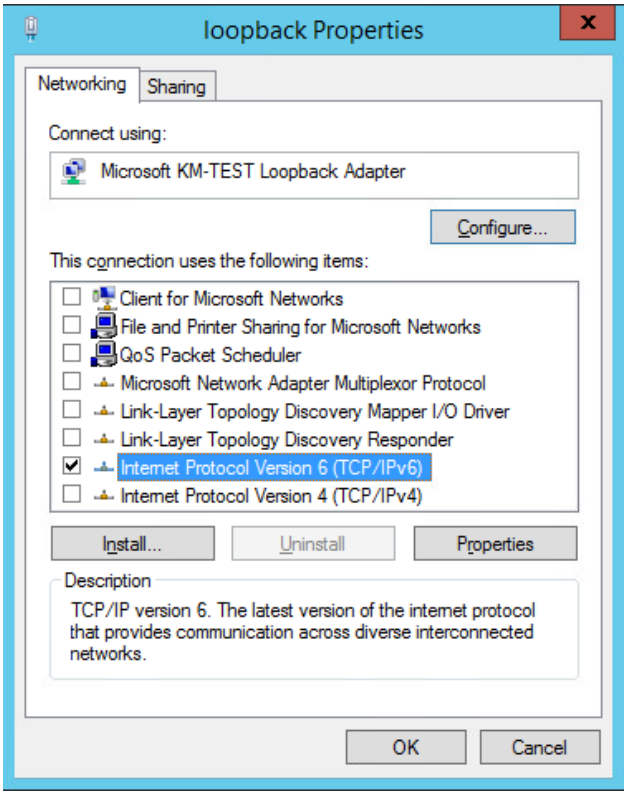
> **Note** **192.168.2.20** is an example, make sure you specify the correct VIP address.

> **Note** If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

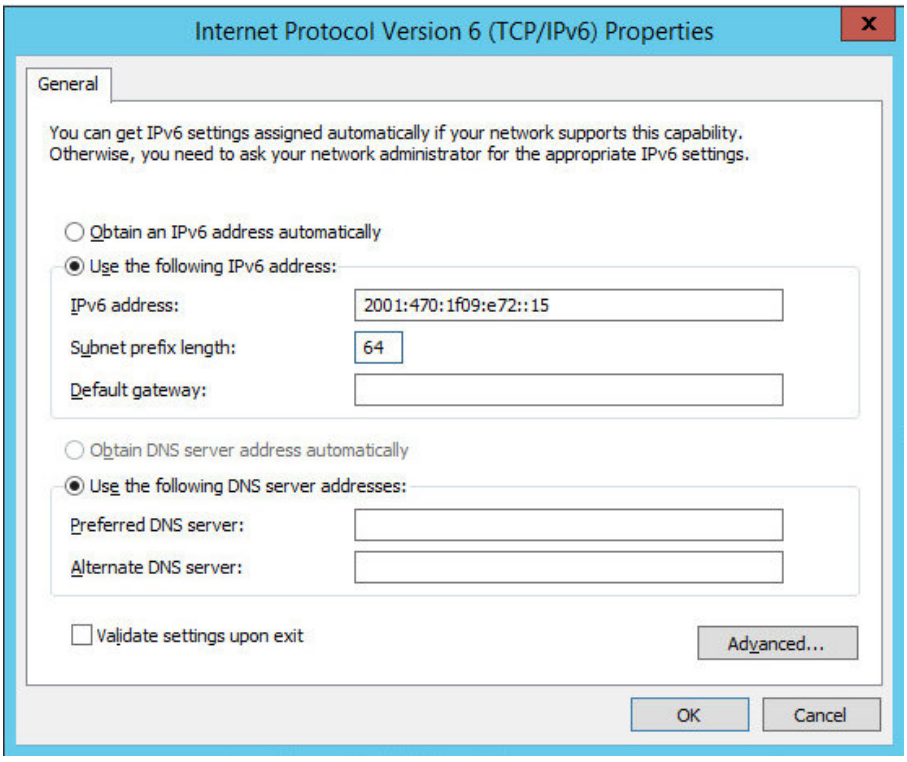
3. Click **OK** then click **Close** to save and apply the new settings.

IPv6 Addresses

1. Uncheck all items except **Internet Protocol Version 6 (TCP/IPv6)** as shown below:



2. Ensure that **Internet Protocol Version (TCP/IPv6)** is selected, 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:



> **Note** **2001:470:1f09:e72::15/64** is an example, make sure you specify the correct VIP address.

> **Note** If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be

added to the Loopback Adapter.

3. Click **OK** then click **Close** to save and apply the new settings.

Step 3 of 3: Configure the strong/weak host behavior

The strong/weak host behavior can be configured using either of the following 2 methods:

- Option 1 - Using network shell (netsh) commands
- Option 2 - Using PowerShell cmdlets

The commands in this section assume that the LAN Adapter is named "**net**" and the Loopback Adapter is named "**loopback**" as shown in the example below:

> **Important** Either adjust the commands to use the names allocated to your LAN and loopback adapters, or rename the adapters before running the commands. Names are case sensitive so make sure that the interface names used in the commands match the adapter names exactly.

Option 1 - Using Network Shell (netsh) Commands

To configure the correct strong/weak host behavior run the following commands:

For IPv4 addresses:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmits=0
```

Option 2 - Using PowerShell Cmdlets

For IPv4 addresses:

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

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

For IPv6 Addresses:

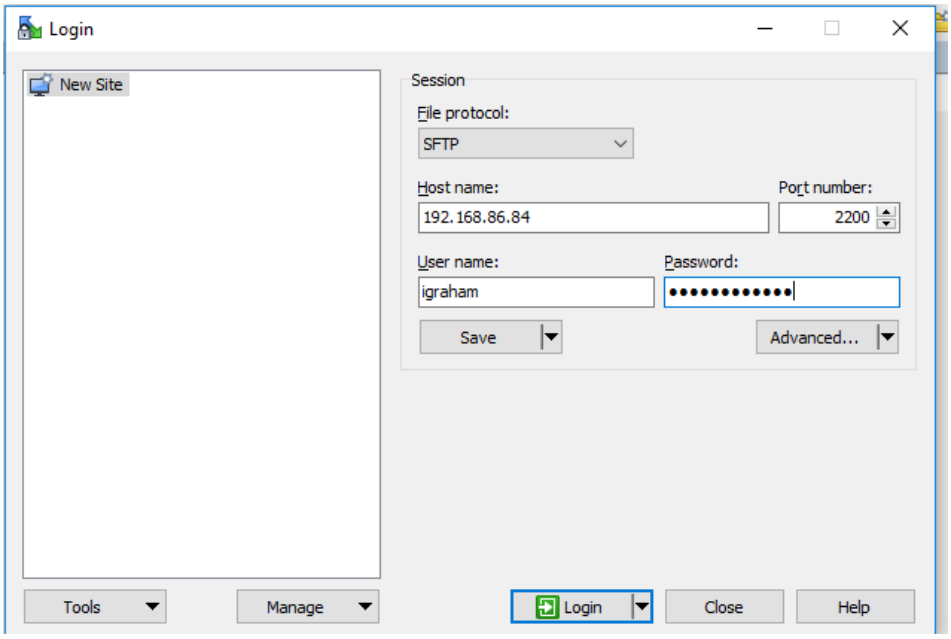
```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv6
```

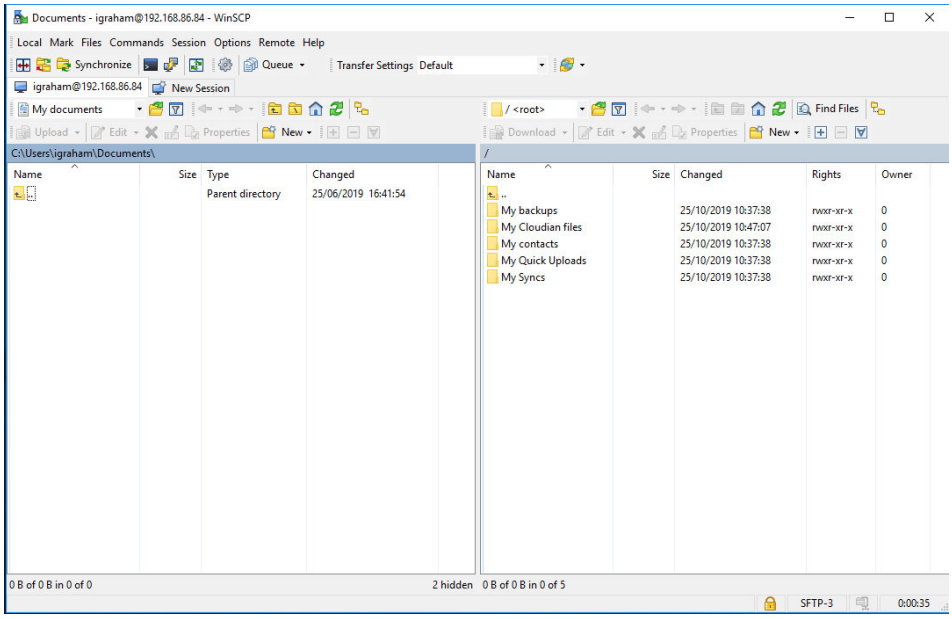
```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6
```

15.2. Testing the SFTP Service

When using SFTP, it should be possible to access the SFTP virtual service using pre-configured SME web portal credentials.

It should be possible to access the SFTP service via the VIP address, by using an SFTP client and appropriate credentials:





The test connection should appear on the System Overview page:

15.3. 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 fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

> **Note** For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library

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.

15.3.1. 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:

WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings

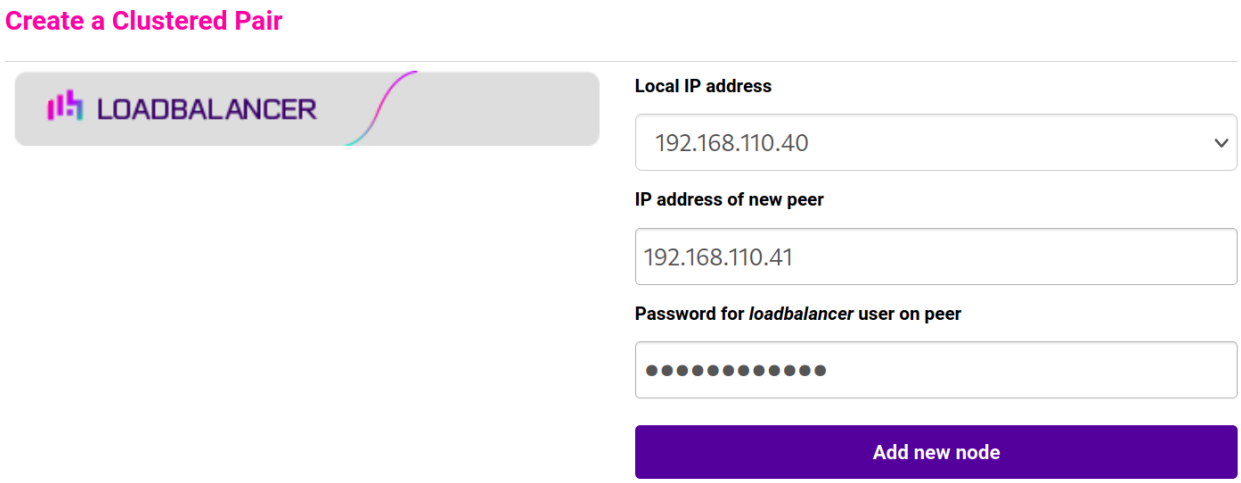
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Fallback Page	Fallback page configuration
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

Important Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

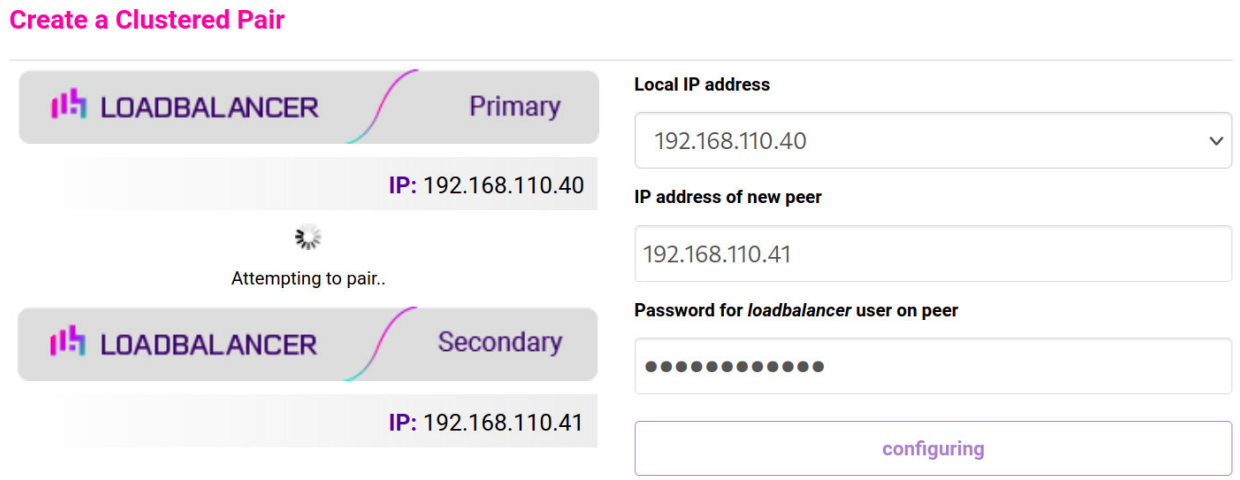
15.3.2. Configuring the HA Clustered Pair

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.

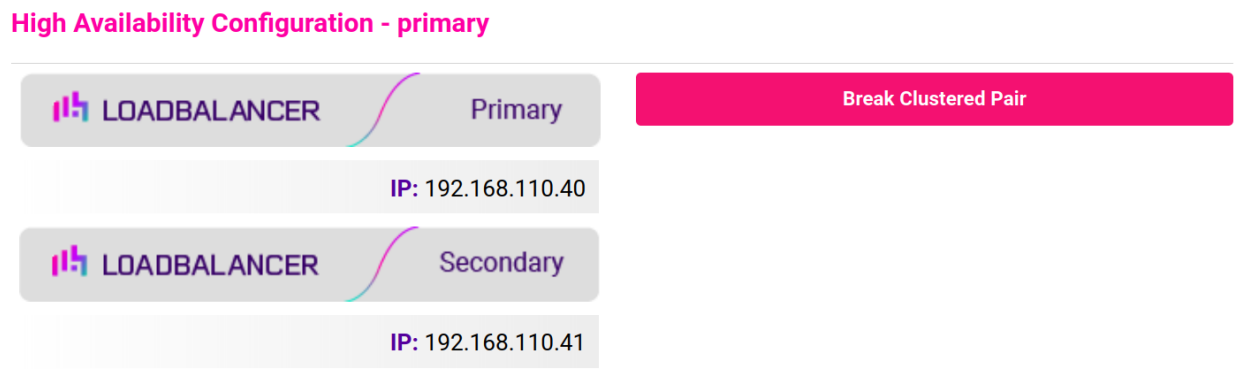
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: ***Cluster Configuration > High-Availability Configuration***.



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:



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



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

> **Note** Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

> **Note** For more details on configuring HA with 2 appliances, please refer to Appliance Clustering for HA.

> **Note** For details on testing and verifying HA, please refer to Clustered Pair Diagnostics.

16. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	17 December 2019	Initial version		IBG, AH
1.0.1	3 September 2020	New title page Updated Canadian contact details	Branding update Change to Canadian contact details	AH
1.1.0	1 December 2021	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.1.1	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.1.2	5 January 2023	Combined software version information into one section Added one level of section numbering Added software update instructions Added table of ports used by the appliance Reworded 'Further Documentation' section Removed references to the colour of certain UI elements	Housekeeping across all documentation	AH
1.1.3	2 February 2023	Updated screenshots	Branding update	AH
1.1.4	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.2.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

LOADBALANCER

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.