1. About this Guide

This guide details the steps required to configure a load balanced Metaswitch Virtual EAS SSS environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Metaswitch Virtual EAS SSS 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 relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Metaswitch Virtual EAS SSS. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td>Enterprise R320</td>
<td>Enterprise 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products/hardware](http://www.loadbalancer.org/products/hardware)

** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- V7.6.4 and later

4. Metaswitch Virtual EAS SSS Software Versions Supported

- Metaswitch Virtual EAS SSS – version 9.x and above
5. Metaswitch Virtual EAS SSS

The following Metaswitch related acronyms are used throughout this document. They are presented here in full for clarity.

- EAS – Enhanced Application Server
- SSS – Stackable Server Solution

This guide specifically describes configuring a virtual load balancer to be used with the deployment of Metaswitch Virtual EAS SSS. The principles and instructions presented here would also apply to a hardware EAS SSS implementation. Loadbalancer.org and Metaswitch have a long-standing partnership for the resale of a fully supported hardware EAS SSS implementation.

In a Metaswitch Virtual EAS SSS deployment, the EAS servers may also be connected to separate signalling and media networks. These additional networks carry SIP and RTP traffic respectively. It is not necessary to connect the load balancer to them as the load balancer is not responsible for load balancing SIP or RTP traffic.

6. Sizing, Capacity, and Performance

For deployments up to 250,000 subscribers, your virtual host should be allocated a minimum of 8 vCPUs, 16 GB of RAM, and 8 GB of disk storage.

This specification will support the following bandwidth and connection thresholds:

- Internet → EAS bandwidth: 100 Mbit/s
- Internet → EAS packets/s: 70,000 pkts/s
- EAS → Internet bandwidth: 700 Mbit/s
- EAS → Internet packets/s: 55,000 pkts/s
- Concurrent connections: 380,000 connections

For larger deployments, your Metaswitch support representative will give you details of the expected load on your load balancers based on your predicted usage profile.

7. Using WAF Gateways

A service provided by a Metaswitch EAS SSS deployment, for example CommPortal access, can be protected with a WAF gateway service on a Loadbalancer.org appliance. This can be done for both virtual and hardware deployments.

A set of five custom WAF rules have been developed to protect a Metaswitch EAS deployment. These rules protect from a range of different attacks, including:

- denial-of-service attacks on login pages
- brute-force attacks to guess passwords
- attempts to gain access to accounts by trying the same common passwords many consecutive times

Instructions on how to deploy WAF gateways, as well as explanations of the custom WAF rules, form a separate deployment guide titled ‘Loadbalancer.org WAF Gateway with Metaswitch EAS’.
8. Load Balancing Metaswitch Virtual EAS SSS

Note: It’s highly recommended that you have a working Metaswitch Virtual EAS SSS environment first before implementing the load balancer.

Persistence (aka Server Affinity)
Some of the virtual services needed to load balance Metaswitch Virtual EAS SSS require source IP persistence.
The EAS servers include a file named pools.txt which describes the virtual services that need to be set up, whether or not they require persistence, and if so what persistence timeout value should be used.
Full instructions on correctly configuring persistence settings can be found in sections Appliance Configuration for Metaswitch Virtual EAS SSS – Two Internal Networks (Scenario 1) and Appliance Configuration for Metaswitch Virtual EAS SSS – One Internal Network (Scenario 2).

Port Requirements
The ports that are load balanced vary from one EAS deployment to another.
The EAS servers include a file named pools.txt which describes the virtual services that need to be set up and which ports they should be listening on.
Full instructions on correctly setting up virtual services listening on the correct ports can be found in sections Appliance Configuration for Metaswitch Virtual EAS SSS – Two Internal Networks (Scenario 1) and Appliance Configuration for Metaswitch Virtual EAS SSS – One Internal Network (Scenario 2).

9. Network Configuration Options
There are two ways that Metaswitch Virtual EAS SSS can be deployed. The deployment type used determines how the load balancer must be configured.
It is essential to know which type of deployment is in place or being planned before attempting to set up a load balancer. If the deployment type is not clear, please contact Metaswitch support for further information.
Scenario 1 – Two Separate Internal Networks (Recommended)

This is the recommended network configuration by Metaswitch. Two separate internal networks are used in this configuration:

- **Service network**: this handles traffic from untrusted external clients, which is load balanced using layer 4 NAT mode virtual services.
- **Management network**: this handles traffic from trusted internal clients, which is load balanced using layer 7 SNAT mode virtual services.

It can be the case that the load balancer needs to be connected to a third separate network, which is the **external network** where traffic from external clients goes to and from. It could also be the case that external traffic flows through a router sitting in either the management or service networks, which removes the need for this third network connection. If it is not clear how external traffic is routed in your deployment, please contact Metaswitch support for further information.

In this type of deployment, traffic flow through the load balancer looks like the following:
There are three main benefits to using two separate internal networks:

- Traffic from external clients, a significant proportion of incoming traffic, can be load balanced using layer 4 NAT mode. This is much faster and less intensive for the load balancer compared to load balancing at layer 7.
- Untrusted external traffic is isolated from the trusted internal management network and traffic.
- Source IP addresses are preserved for incoming requests from external clients, i.e. clients out on the public Internet. This makes identifying and blocking malicious clients easier.

Note: It is possible to use two separate HA pairs of load balancers in this scenario.

In this case, the first pair of load balancers would connect the external clients to the service network, and would host layer 4 NAT mode VIPs. The second pair of load balancers would sit in the internal trusted management network, and would only load balance internal traffic using layer 7 VIPs.

In practice, the functionality of these two HA pairs of load balancers can be combined into a single pair, provided that they have ‘arms’ in each of the necessary networks (the service network, management network, and external network too if applicable).

This guide describes setting up a single HA pair of load balancers.
Scenario 2 – One Internal Network

An EAS deployment can be built without a separate service network. In this case, external and internal traffic is all handled on a single internal network. All traffic must be load balanced using layer 7 SNAT mode virtual services.

When load balancing at layer 7, performance is not as fast as the layer 4 option available in scenario 1. Layer 7 load balancing is also more intensive for the load balancer.

The load balancer acts as a full proxy in this setup, and as such load balancing is not source IP transparent. This means the EAS servers see all inbound traffic as originating from one of the load balancer’s IP addresses. This makes it difficult to identify and block malicious requests from external clients on the public Internet, as their source IP addresses are obscured.
Virtual Service (VIP) Requirements
The number of virtual services required on the load balancer varies between Metaswitch Virtual EAS SSS deployments. The EAS writes a file named pools.txt which details every virtual service that needs to be configured. This file can be found on any EAS server, in the directory /home/defcraft/files.

Instructions on how to configure these virtual services can be found in the following sections, depending on which network configuration / scenario you are using:
- Appliance Configuration for Metaswitch Virtual EAS SSS – Two Internal Networks (Scenario 1)
- Appliance Configuration for Metaswitch Virtual EAS SSS – One Internal Network (Scenario 2)

Load Balancing Methods
The load balancer can be deployed in one of 4 fundamental ways: Layer 4 DR mode, Layer 4 NAT mode, Layer 4 SNAT mode, or Layer 7 SNAT mode. For Metaswitch Virtual EAS SSS, layer 4 NAT mode and layer 7 SNAT mode virtual services are supported. Both of these supported load balancing methods are described below.

Layer 4 NAT Mode
Layer 4 NAT (network address translation) mode is a high performance solution.

- 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.

• In a Metaswitch Virtual EAS SSS deployment, NAT mode is deployed in one of the following ways:

2-arm (using 2 Interfaces), 2 subnets (as shown above) - One interface on the load balancer is connected to the internal management network and the second interface is connected to the internal service network. The NAT mode VIP is brought up so that it is accessible to external traffic, which could be on the service network or a separate external network if needed. The default gateway on the EAS servers is set to be an IP address in the service network on the load balancer. This is configured on the EAS servers, and the IP address to be used should be known prior to EAS commissioning.

External clients or clients in any remote subnet can use this virtual service, 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.

• NAT mode is transparent, i.e. the Real Server will see the source IP address of the client. This is useful for the EAS servers, as this allows blocking the IP addresses of malicious users on the public Internet.

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

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 request to the chosen Real Server. As a result, Layer 7 is a slower technique than NAT mode at Layer 4. 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.

In the case of a Metaswitch Virtual EAS SSS deployment, layer 7 load balancing must be used for traffic on the internal management network, where the clients sit in the same subnet as the real servers. If using scenario 2, where only a single internal network is used, then layer 7 load balancing must be used for all traffic, both from external and internal sources.
This mode can be deployed in a one-arm or two-arm configuration and does not require any changes to the Real Servers. However, since the load balancer is acting as a full proxy it doesn’t have the same raw throughput as the layer 4 methods.

The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

- SNAT mode is a full proxy and therefore load balanced Real Servers do not need to be changed in any way
- Because SNAT mode is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN
- 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 balancers 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

SNAT mode can be deployed using either a 1-arm or 2-arm configuration.
Virtual Appliance Download & Deployment

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 and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB 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 Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Initial Network Configuration

The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

**Method 1 - Using the Network Setup Wizard at the console**

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

**Method 2 - Using the WebUI**

Using a browser, connect to the WebUI on the default IP address/port: https://192.168.2.21:9443

To set the IP address & subnet mask, use: Local Configuration > Network Interface Configuration

To set the default gateway, use: Local Configuration > Routing

To configure DNS settings, use: Local Configuration > Hostname & DNS

**Accessing the Web User Interface (WebUI)**

The WebUI can be accessed via HTTPS at the following URL: https://192.168.2.21:9443/lbadmin
* Note the port number → 9443

(replace 192.168.2.21 with the IP address of your load balancer if it’s been changed from the default)

Login using the following credentials:

- **Username**: loadbalancer
- **Password**: loadbalancer

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

Once logged in, the WebUI will be displayed as shown on the following page:
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 section 4 of the appendix on page 34.
11. Appliance Configuration for Metaswitch Virtual EAS SSS – Two Internal Networks (Scenario 1)

Two separate internal networks are used in this scenario.

During initial setup, the load balancer should have been assigned an IP address on the trusted internal management network. This IP address is assigned to the eth0 network interface. With this IP address, the load balancer has an ‘arm’/connection set up to the trusted internal management network.

The load balancer must now be given an arm in the internal service network, as well as an arm in the external network if that is a separate network.

Connecting the Load Balancer to the Service Network

The load balancer needs to be assigned an IP address in the service network to use that network. This IP address should be assigned to a separate network interface.

To assign an IP address from the WebUI:

1. Go to Local Configuration > Network Interface Configuration
2. Add the required IP address and subnet mask next to the appropriate NIC under IP Address Assignment
3. Press the Configure Interfaces button

In the example presented here, the IP address 192.168.85.240/18, which sits in the service network, is being added to interface eth1:
Note: If the load balancer is being set up as part of a highly available pair, the slave load balancer must also be assigned its own IP address in the service network by following the same steps.

Connecting the Load Balancer to the External Network
The load balancer must have an ‘arm’ in the external network through which client traffic enters the EAS deployment. How this is accomplished will depend on how the network is set up.

For some deployments, external client traffic enters through a firewall/router that sits in the service network. In this situation, if the external facing firewall can be reached from the load balancer’s IP address in either the management network or the service network then no additional configuration is necessary.

If external client traffic enters the deployment from a third distinct network then the load balancer will need an arm / IP address in that network. To do this, follow the same steps used in the previous section Connecting the Load Balancer to the Service Network. A third NIC can be used for this, e.g. eth2.

Configuring the Virtual Services
A list of every virtual service that needs to be configured on the load balancer can be found on any of the EAS servers (the list files are identical). The EAS writes this list to the file pools.txt. This file can be found on any EAS server in the directory /home/defcraft/files.

Configuring The Layer 7 Management VIPs
The first section of the pools.txt file is headed “Management”. It describes the VIPs that need to be set up on the internal management network. These are all layer 7 SNAT mode VIPs. This section of the file looks like this:

<table>
<thead>
<tr>
<th>POOL</th>
<th>POOL IP</th>
<th>PROTO</th>
<th>PORT</th>
<th>STICKY</th>
<th>SERVER IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td># MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP-143</td>
<td>10.225.37.223</td>
<td>tcp</td>
<td>143</td>
<td>0</td>
<td>10.225.37.231 10.225.37.116</td>
</tr>
</tbody>
</table>

Each line after the “Management” heading describes an individual VIP to be set up. These lines are read as follows:

- **Pool**: a descriptive name for the VIP, which could be used as the VIP label on the load balancer
- **Pool IP**: the IP address that must be used for the virtual service
- **Proto**: the protocol for the virtual service, which should always be listed as TCP
- **Port**: the port that must be used for the virtual service
- **Sticky**: the source IP persistence setting to be used. A value of 0 means persistence must be disabled. A non-zero value means source IP persistence must be enabled and have a timeout equal to that number of seconds
• **Server IPs**: the RIs (IP addresses of each real server) that must be added to the VIP

Every layer 7 virtual service described in the file needs to be set up. Instructions on how to set up a layer 7 VIP are presented below.

**Configuring a Layer 7 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 desired, e.g. MGMT_HTTPS-443
3. Set the **Virtual Service IP Address** field to the “Pool IP” value, e.g. 10.225.37.227
4. Set the **Ports** field to the “Port” value, e.g. 443
5. Set the **Layer 7 Protocol** to **TCP Mode**
6. Click **Update** to create the virtual service

```
<table>
<thead>
<tr>
<th>Layer 7 - Add a new Virtual Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
</tr>
<tr>
<td>Virtual Service IP Address</td>
</tr>
<tr>
<td>Ports</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
</tr>
<tr>
<td>Manual Configuration</td>
</tr>
</tbody>
</table>
```

7. Click **Modify** next to the newly created VIP
8. Set **Balance Mode** to **Weighted Round Robin**
9. Set **Persistence Mode** as required:
   - If the “Sticky” column has a value of 0 then **Persistence Mode** must be set to **None**
   - If the “Sticky” column has a non-zero value then **Persistence Mode** must be set to **Source IP** and the **Persistence Timeout** must be set equal to the “Sticky” value divided by 60. The division is necessary because the layer 7 persistence timeout units are minutes as opposed to the ‘Sticky’ units which are seconds
10. Set **Health Checks** to **Connect to port**
11. Set **Check Port** to the “Port” value, e.g. 443
12. Under the **Other** section, click the **Advanced** button
13. Check the **Timeout** checkbox
14. Set the **Client Timeout** value to 900000
15. Set the **Real Server Timeout** value to 901000
16. Click **Update**

**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. **EAS_SSS-1**.
3. Set the **Real Server IP Address** field to the first “Server IPs” value, e.g. **10.225.37.231**.
4. Set the **Real Server Port** field to the “Port” value, e.g. **443**.
5. Click **Update**.
6. Repeat these steps until all the listed EAS servers have been added.

![Layer 7 Add a new Real Server - MGMT_HTTPS-443](image)

**Changing Layer 7 Global Settings**

Once all of the individual VIPs have been set up, one of the layer 7 global settings needs to be changed.

1. From the WebUI, go to *Cluster Configuration > Layer 7 – Advanced Configuration*.
2. Set **Interval** to **3000**.
3. Click **Update**.

**Finalizing the Layer 7 Configuration**

To apply the new settings, HAProxy must be restarted as follows:

1. Using the WebUI, navigate to: **Maintenance > Restart Services** and click **Restart HAProxy**.

**Configuring The Layer 4 Service VIPs**

The second section of the pools.txt file is headed “Service”. It describes the VIPs that need to be set up on the internal service network. These are all layer 4 NAT mode VIPs. This section of the file looks like this:
# SERVICE

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>VIP Address 1</th>
<th>VIP Address 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP-80</td>
<td>tcp</td>
<td>80</td>
<td>192.168.85.61</td>
<td>192.168.85.5</td>
</tr>
<tr>
<td>HTTPS-443</td>
<td>tcp</td>
<td>443</td>
<td>192.168.85.61</td>
<td>192.168.85.5</td>
</tr>
<tr>
<td>HTTPS-10000</td>
<td>tcp</td>
<td>10000</td>
<td>192.168.85.61</td>
<td>192.168.85.5</td>
</tr>
<tr>
<td>IMAP-143</td>
<td>tcp</td>
<td>143</td>
<td>192.168.85.61</td>
<td>192.168.85.5</td>
</tr>
</tbody>
</table>

Each line after the “Service” heading describes an individual VIP to be set up. These lines are read in the same way as the “Management” VIPs, and a list of descriptions of each column can be found on page 17.

Every layer 4 virtual service described in the file needs to be set up. Instructions on how to set up a layer 4 VIP are presented below.

Configuring a Layer 4 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 desired, e.g. SERV.IMAP-143
3. Set the **Virtual Service IP Address** field to an IP address of your choice, bearing in mind the following two conditions for NAT mode to work:
   - The VIP address must be accessible from the external network
   - The VIP address must be in a different subnet to the real server IP addresses
   In this example the VIP address 192.168.85.150 is used, as this IP address is not in the same subnet as the example real servers which are sitting in the 192.168.85.0/25 subnet
4. Set the **Ports** field to the “Port” value, e.g. 143
5. Set the **Protocol** to **TCP**
6. Set the **Forwarding Method** to **NAT**
7. Click **Update** to create the virtual service

8. Click **Modify** next to the newly created VIP
9. Set Balance Mode to Weighted Round Robin

10. Set Persistent as required:
   - If the “Sticky” column has a value of 0 then the Persistent checkbox must not be checked
   - If the “Sticky” column has a non-zero value then the Persistent checkbox must be checked and the Persistence Timeout must be set to the “Sticky” value (the layer 4 persistence timeout units are seconds, so no division is necessary as it is layer 7 services)

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. EAS_SSS-1
3. Set the Real Server IP Address field to the first “Server IPs” value, e.g. 192.168.85.61
4. Click Update
5. Repeat these steps until all the listed EAS servers have been added

![Layer 4 Add a new Real Server - SERV.IMAP-143](image)

Changing Layer 4 Global Settings

Once all of the individual VIPs have been set up, some of the layer 4 global settings regarding health checking need to be changed.

1. From the WebUI, go to Cluster Configuration > Layer 4 – Advanced Configuration
2. Set Check Interval to 3
3. Set Check Timeout to 3
4. Set Failure Count to 2
5. Click Update
Creating a Floating IP Address on the Service Network

If deploying an HA pair of load balancers, a floating IP address sitting on the service network must be created on the load balancers.

Because of how layer 4 NAT mode works, the EAS servers must have their gateway for the service network set to be an IP address that is owned by the load balancer. This causes the EAS servers to reply to incoming service network traffic via the load balancer. The gateway is configured on the EAS servers, and the IP address to be used for this must be known prior to EAS commissioning. Instructions for confirming the gateways configured on an EAS server are presented in Appendix 1, Confirming the Gateway Settings on the EAS Servers, on page 29.

For a pair of load balancers, the gateway IP address must be a floating IP address. This means that during a fail over from one load balancer to the other this IP address is picked up by the other appliance, enabling traffic to continue to route from the real servers on toward the external clients.

To add the floating IP address from the WebUI on the master load balancer:

1. Navigate to Cluster Configuration > Floating IPs
2. Specify the new floating IP addresses
3. Click the Add Floating IP button

12. Appliance Configuration for Metaswitch Virtual EAS SSS – One Internal Network (Scenario 2)

A single internal network is used in this scenario. All traffic is handled by a single set of layer 7 virtual services, traffic from both from internal clients and external clients out on the Internet.

Configuring the Virtual Services

A list of every virtual service that needs to be configured on the load balancer can be found on any of the EAS servers (the list files are identical). The EAS writes this list to the file pools.txt. This file can be found on any EAS server in the directory /home/defcraft/files.
Configuring The Layer 7 Management VIPs

If the EAS servers are configured for use in a single internal network environment, the pools.txt file should contain a single section headed “Management”. It describes the layer 7 VIPs that need to be set up. These are all layer 7 SNAT mode VIPs. The file looks like this:

<table>
<thead>
<tr>
<th>POOL</th>
<th>POOL IP</th>
<th>PROTO</th>
<th>PORT</th>
<th>STICKY</th>
<th>SERVER IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td># MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP-143</td>
<td>10.225.37.223</td>
<td>tcp</td>
<td>143</td>
<td>0</td>
<td>10.225.37.231 10.225.37.116</td>
</tr>
</tbody>
</table>

Each line after the “Management” heading describes an individual VIP to be set up. These lines are read as follows:

- **Pool**: a descriptive name for the VIP, which could be used as the VIP label on the load balancer
- **Pool IP**: the IP address that must be used for the virtual service
- **Proto**: the protocol for the virtual service, which should always be listed as TCP
- **Port**: the port that must be used for the virtual service
- **Sticky**: the source IP persistence setting to be used. A value of 0 means persistence must be disabled. A non-zero value means source IP persistence must be enabled and have a timeout equal to that number of seconds
- **Server IPs**: the RIPv (IP addresses of each real server) that must be added to the VIP

Every layer 7 virtual service described in the file needs to be set up. Instructions on how to set up a layer 7 VIP are presented below.

Configuring a Layer 7 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 desired, e.g. **MGMT_HTTPS-443**
3. Set the Virtual Service IP Address field to the “Pool IP” value, e.g. **10.225.37.227**
4. Set the Ports field to the “Port” value, e.g. **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 **Balance Mode** to **Weighted Round Robin**.
9. Set **Persistence Mode** as required:
   - If the "Sticky" column has a value of 0 then **Persistence Mode** must be set to **None**.
   - If the "Sticky" column has a non-zero value then **Persistence Mode** must be set to **Source IP** and the **Persistence Timeout** must be set equal to the "Sticky" value divided by 60. The division is necessary because the layer 7 persistence timeout units are minutes as opposed to the 'Sticky' units which are seconds.
10. Set **Health Checks** to **Connect to port**.
11. Set **Check Port** to the "Port" value, e.g. **443**.
12. Under the **Other** section, click the **Advanced** button.
13. Check the **Timeout** checkbox.
14. Set the **Client Timeout** value to **900000**.
15. Set the **Real Server Timeout** value to **901000**.
16. Click **Update**.

### 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. **EAS_SSS-1**.
3. Set the **Real Server IP Address** field to the first "Server IPs" value, e.g. **10.225.37.231**.
4. Set the **Real Server Port** field to the "Port" value, e.g. **443**.
5. Click **Update**.
6. Repeat these steps until all the listed EAS servers have been added.
Changing Layer 7 Global Settings

Once all of the individual VIPs have been set up, one of the layer 7 global settings needs to be changed.

1. From the WebUI, go to Cluster Configuration > Layer 7 – Advanced Configuration
2. Set Interval to 3000
3. Click Update

Finalizing the Layer 7 Configuration

To apply the new settings, HAProxy must be restarted as follows:

1. Using the WebUI, navigate to: Maintenance > Restart Services and click Restart HAProxy

13. Testing & Verification

Metaswitch Specific Tests

Metaswitch recommend using some specific tests which make use of the EAS Craft menu and the CommPortal web portal.

Pool Configuration Test

Metaswitch provide a Python test script which reads the pools.txt file and checks that each virtual service has been created correctly and is accepting connections. This script can be run on any Linux or Windows machine that has Python 2.7 installed and can access the appropriate networks for the deployment.

The following points should be considered before running the test:

- At least one EAS server must be running for a successful test
- Depending on the network configuration, the script may need to be run separately from two different machines to test both the internal ‘management network’ services and the external facing ‘service network’ services
- If ‘service network’ services have been set up, the script will ask for the IP address and port that has been assigned for each virtual service, as these are set by the user and are not pre-defined
The test script must not be run from an EAS server, as this will return false positives for all tests.

Running the Test

1. Copy the Python script to an appropriate test machine
2. Put the script in the same directory as the pools.txt file
3. Run the test by executing the following, either from a Linux shell or the Windows command prompt:
   ```
   python testpools.py
   ```
4. Follow the script's prompts and make sure that both the management and the service network virtual services are tested if testing a deployment that uses two internal networks (otherwise only the management services will have been set up and these should be tested)
5. Address any reported errors by checking the configuration of any problematic virtual services on the load balancer.

Health Checking Test

This test is disruptive to end users and should not be run on a live production system.

This test verifies that the load balancer’s real server health checking is correctly configured. When an EAS server goes offline the load balancer should detect this change.

1. Ensure that all EAS servers are online
2. Open the System Overview page of the load balancer’s WebUI
3. Check that all virtual services and real servers are displayed as online/green
4. Use the EAS Craft interface to stop the software services on one or more real servers, by navigating to Main > Manage servers and passwords > Stop a server
5. Check the load balancer’s System Overview page again, and verify that after a few seconds the appropriate EAS servers are now displayed as offline/red
6. Use the EAS Craft interface to start all servers, by navigating to Main > Manage servers and passwords > Start ALL servers
7. Check the load balancer’s System Overview page again, and verify that after a few seconds all virtual services and real servers are now displayed as online/green

Persistence Test

This test is disruptive to end users and should not be run on a live production system.

This test verifies that persistence is configured correctly. For virtual services with persistence enabled, an end user should be load balanced to the same EAS server until their persistence session/entry times out.

Metaswitch note that this test doesn't have to be conducted for every virtual service with persistence enabled (i.e. services with non-zero "STICKY" values in pools.txt), and that provided the test works for one virtual service, and that other 'sticky' services are configured in the same way, this is sufficient.

1. Use the EAS Craft interface to stop approximately half of the EAS servers, making sure that at least one is left running. Do this by navigating to Main > Manage servers and passwords > Stop a server
2. Use a browser to access the CommPortal web interface via one of the configured virtual services (one of HTTP-80, HTTPS-443, HTTPS-100XX)
3. Log in using a test account
4. Once successfully logged in, start up all servers by navigating to Main > Manage servers and passwords > Start ALL servers
5. Return to the CommPortal session, click on some of the tabs, and press Ctrl+F5 several times to force reload the page. The log in session should persist without issue
6. Use the EAS Craft interface to stop all of the EAS servers that were left running at the start of this test, by navigating to Main > Manage servers and passwords > Stop a server
7. Return to the CommPortal session and press Ctrl+F5 to force reload the page. The test user should now be logged out, and the login screen should be displayed again.
8. Log back in using the test account, and then press Ctrl+F5 several times to force reload the page. The log in session should persist without issue
9. Start up all servers again by navigating to Main > Manage servers and passwords > Start ALL servers
10. Return to the CommPortal session and press Ctrl+F5 several times to force reload the page. The log in session should persist without issue. The test is now complete

Fail Over / High Availability Test

This test is disruptive to end users and should not be run on a live production system.

If using a highly available pair of load balancers, the fail over functionality between them can be tested.

1. Log into the CommPortal web interface
2. Trigger a fail over from your active load balancer to your passive load balancer. You could force this by powering off the active load balancer
3. Press Ctrl+F5 in browser to force refresh the CommPortal page
4. Once a successful fail over has taken place, the passive load balancer will become active and will start serving traffic. The browser should show the CommPortal again. Note that a new log in may need to be performed following a fail over

Useful Load Balancer Based Checks

Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPS (i.e. the EAS servers) and shows the state/health of each server as well as the state of the each cluster as a whole. The example below shows that all EAS servers are healthy and available to accept connections.
14. Technical Support
For more details about configuring the appliance and assistance with designing your deployment please don’t hesitate to contact the support team using the following email address: support@loadbalancer.org

15. Further Documentation

16. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Metaswitch Virtual EAS SSS environments.
17. Appendix

1 – Confirming the Gateway Settings on the EAS Servers

It is possible to confirm what network gateways are defined on an EAS server. If a gateway needs to be changed to enable load balancing to work correctly, please contact Metaswitch support for assistance with this.

Confirming the gateway settings is done using the EAS Craft interface like so:

1. Sign into the EAS Craft interface
2. Select option 1, Configuration

```
Craft on svr01 (lbsdc)
Version V9.4.20-02
WARNING: svr01 is unlicensed
[Main]
Main menu

ENTER   Refresh
0)   < Log off the craft menu
1)   > Configuration
2)   > Manage software version
3)   > Manage servers and passwords
4)   > Diagnostics and recovery
5)   > Web configuration
6)   > Administration
8)   > TUI Customizations

Select an item: 1
```

3. Select option 2, Network parameters

```
Craft on svr01 (lbsdc)
Version V9.4.20-02
WARNING: svr01 is unlicensed
[Main->Config]
Configuration

ENTER   Refresh
0)   < Back to previous menu
1)   > EAS parameters
2)   > Network parameters
3)   > Configure EAS services
4)   > Configure EAS servers
5)   > Configure 3rd-party hardware
6)   > Service Federation configuration
7)   > Manage TUI language packs
8)   > Licensing

Select an item: 2
```
4. Select option 6, Manage subnets

Craft on srv01 (lbsdc)
Version V9.4.20-02
WARNING: srv01 is unlicensed
[Main->Config->Network]
Network parameters

ENTER Refresh
0) < Back to previous menu
1) > SIP Settings
2) > NTP, DNS, and rsyslog servers
3) > Trusted Networks
4) > MetaView Network Config
5) > Server IP addresses and UDP multicast configuration
6) > Manage subnets
7) > External Servers

Select an item: 6

5. Select option 1, List all subnets

Craft on srv01 (lbsdc)
Version V9.4.20-02
WARNING: srv01 is unlicensed
[Main->Config->Network->Subnet]
Manage subnets

ENTER Refresh
0) < Back to previous menu
1) List all subnets

Select an item: 1

6. The different gateways configured on the server are listed. In the example presented here, the IP address 172.60.5.60 (highlighted) is used for the gateway on the service network.

In the example deployment in question, a floating IP address of 172.60.5.60 is configured on the load balancer pair to enable traffic to flow correctly.
2 – Full Configuration Backup

When using a third party load balancer in a Metaswitch Virtual EAS SSS deployment, taking backups of the load balancer is an exercise that is left to the user.

Having a full configuration backup is very useful. In the unlikely event of a catastrophic failure, a fresh load balancer could be quickly deployed and put into production. In another scenario, if the load balancer’s configuration were altered and broken in the future then the backed up working configuration could be imported and restored.

Taking A Backup

Once a load balancer has been fully deployed, configured, and is working as intended, it is very easy to take a full configuration backup.

1. From the WebUI, navigate to Support > Technical Support Download
2. Click the Generate Archive button
3. Wait for the archive to be generated
4. Use the download link to save the archive to a safe location

Restoring From A Backup

A support download archive contains an XML file (lb_config.xml) which describes the appliance’s setup. This XML file can be imported into a load balancer to restore the backed up configuration.

1. From the WebUI, navigate to Maintenance > Backup & Restore > Restore Tab
2. Use the Upload XML file & Restore function
3. Wait for the success message that the configuration has been fully restored

Note that a support download is also an invaluable tool for diagnosing problems with a load balancer, as it contains configuration and log files.
3 – Performing Updates With Minimal Downtime

With a highly available pair of load balancers, it is possible to perform updates to the load balancers with a minimal amount of downtime.

Presented below are our full instructions on how to safely update a pair of load balancers with minimal disruption to load balanced services and clients.

Online and offline update options are both possible and are described below.

General Guidance for Performing Updates

- **Maintenance window**: since services may be restarted during the update process, we recommend performing the update during a maintenance window.

- **Updates are incremental**: if you wish to perform several updates in one window, we recommend installing each update in turn, ignoring calls to restart services or reboot the appliance until all available updates have been installed and the appliance is fully up to date.

- **Backups**: we recommend that you backup your XML configuration and firewall script (if changes have been made) before running an update. Do this by using the buttons in the web interface, under Maintenance > Backup & Restore.

Specific Guidance for Updating a Clustered Pair of Load Balancers

1. Perform the update on the passive appliance first, which is usually the slave. The updates are incremental, so we recommend installing each update in turn, ignoring calls to restart services or reboot the appliance until all available updates have been installed and the appliance is fully up to date.

2. Next, restart services or reboot the appliance as directed.

3. Fail over to the updated appliance so that it becomes the active appliance.

4. Now update the other unit in the same way.

   - For a clustered pair, we strongly recommend fully testing & validating the master/slave fail-over process before going live. If testing was not carried out before go-live, we recommend scheduling a maintenance window to do this. For detailed steps, please refer to the Administration Manual.

Online Updates

To perform an online update:

- Ensure the load balancer can access the Internet (requires a valid default gateway and DNS server to be set).

- In the web interface, open Maintenance > Software Update.

- Select Online Update.

- If an update is available, information about the update will be displayed.

- Click the Online Update button.

- Once complete (the update can take several minutes depending on download speed and upgrade version), the message ‘Update completed successfully’ will be displayed.

- If there are any specific post-upgrade requirements, such as a service restart, these will be displayed on the screen after the installation completes.
Offline Updates

To perform an offline update:

- In the web interface, open Maintenance > Software Update
- Select Offline Update
- Select the correct matching update archive and checksum files
- Click Upload and Install
4 – Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

Note: A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
- Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
- SNMP settings
- Graphing settings
- Firewall Script & Firewall Lockdown Script settings
- Software updates

Version 7:

Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8:

To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration
• Specify the IP address and the loadbalancer users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above

• Click Add new node

• The pairing process now commences as shown below:

• Once complete, the following will be displayed:

• To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the
Note: Clicking the Restart Heartbeat button on the master appliance will also automatically restart heartbeat on the slave appliance.

Note: Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
### 18. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>10 May 2018</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>24 May 2018</td>
<td>Total re-write, based on Metaswitch's load balancing document sent over on the back of the initial version</td>
<td>Document re-write</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.2</td>
<td>5 June 2018</td>
<td>Changed 'Metaswitch EAS SSS' to 'Metaswitch Virtual EAS SSS' at Metaswitch's request</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added a paragraph saying that although the guide is for virtual it still applies to hardware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.3</td>
<td>6 August 2018</td>
<td>Corrected the layer 7 persistence timeout instructions, as the units are minutes while Metaswitch customers will have a list of timeouts to input that are in seconds</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added a new Appendix 1, 'Confirming the Gateway Settings on the EAS Servers'</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed 'Pool Configuration Test' paragraph to remove reference to using Python 3.x; Metaswitch have advised running the script with Python 2.7 only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corrected the System Overview screenshot under 'Useful Load Balancer Based Checks' where the MGMT_HTTP-80 VIP was erroneously in HTTP Mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.4</td>
<td>19 September 2018</td>
<td>Added section 6, “Sizing, Capacity, and Performance”</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.5</td>
<td>27 September 2018</td>
<td>Added section 7, “Using WAF Gateways”</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.6</td>
<td>6 December 2018</td>
<td>Added the new “Company Contact Information” page</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>15 August 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated the advice in section 7, &quot;Using WAF Gateways&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>****</td>
<td>Added a paragraph describing layer 4 health check timeout changes, to bring them in line with the layer 7 health check settings</td>
<td>****</td>
<td></td>
<td></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.

United Kingdom
Loadbalancer.org Ltd.
Compass House, North Harbour Business Park, Portsmouth, PO6 4PS
UK: +44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

Canada
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver,
BCV6B 2Z4, Canada
TEL: +1 302.213.0122
sales@loadbalancer.org
support@loadbalancer.org

United States
Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

Germany
Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org