Load Balancing Dell EMC ECS

v1.1.2
Contents

1. About this Guide .................................................................................................................................................. 4
2. Loadbalancer.org Appliances Supported ........................................................................................................... 4
3. Loadbalancer.org Software Versions Supported ............................................................................................... 4
4. Dell EMC ECS Software Versions Supported .................................................................................................... 4
5. Dell EMC ECS .................................................................................................................................................... 5
6. Load Balancing Dell EMC ECS ........................................................................................................................... 5
   Persistence (aka Server Affinity) .......................................................................................................................... 5
   Virtual Service (VIP) Requirements .................................................................................................................... 5
   Port Requirements .............................................................................................................................................. 5
   TLS/SSL Termination .......................................................................................................................................... 6
   Health Checks .................................................................................................................................................... 6
   S3, Atmos, and Swift Virtual Services ................................................................................................................ 6
   NFS Virtual Service .......................................................................................................................................... 6
7. Deployment Concept .............................................................................................................................................. 7
   Scenario 1 – Virtual Services for Each Protocol ................................................................................................ 7
   Method A: Sorting by Port .................................................................................................................................. 7
   Method B: Sorting by IP Address ........................................................................................................................ 8
   Scenario 2 – Single Client-facing Virtual Service ............................................................................................ 8
   Helping you Choose the Most Appropriate Deployment Type ............................................................................. 9
8. Loadbalancer.org Appliance – the Basics ........................................................................................................... 10
   Virtual Appliance Download & Deployment ...................................................................................................... 10
   Initial Network Configuration .............................................................................................................................. 10
   Accessing the Web User Interface (WebUI) .......................................................................................................... 10
   HA Clustered Pair Configuration ........................................................................................................................ 12
9. Appliance Configuration for Dell EMC ECS – Scenario 1 ................................................................................ 13
   Changing the Global Layer 7 Settings .................................................................................................................. 13
   Configuring VIP 1 – S3 ....................................................................................................................................... 13
      Configuring the Virtual Service (VIP) ................................................................................................................ 13
      Defining the Real Servers (RIPS) ....................................................................................................................... 14
   Configuring VIP 2 – Atmos .................................................................................................................................. 14
      Configuring the Virtual Service (VIP) ................................................................................................................ 14
      Defining the Real Servers (RIPS) ....................................................................................................................... 15
   Configuring VIP 3 – Swift ................................................................................................................................... 16
      Configuring the Virtual Service (VIP) ................................................................................................................ 16
      Defining the Real Servers (RIPS) ....................................................................................................................... 16
   Configuring VIP 4 – NFS .................................................................................................................................... 17
      Configuring the Virtual Service (VIP) ................................................................................................................ 17
      Defining the Real Servers (RIPS) ....................................................................................................................... 18
   Finalizing the Configuration ............................................................................................................................... 19
10. Appliance Configuration for Dell EMC ECS – Scenario 2 .............................................................................. 19
    Changing the Global Layer 7 Settings ................................................................................................................ 19
    Configuring VIP 1 – S3 ....................................................................................................................................... 19
    Configuring the Virtual Service (VIP) ................................................................................................................ 19
Defining the Real Servers (RIPs).................................................................................................................. 20
Configuring VIP 2 – Atmos............................................................................................................................... 21
Configuring the Virtual Service (VIP)............................................................................................................. 21
Defining the Real Servers (RIPs).................................................................................................................. 22
Configuring VIP 3 – Swift............................................................................................................................... 23
Configuring the Virtual Service (VIP)............................................................................................................. 23
Defining the Real Servers (RIPs).................................................................................................................. 23
Configuring VIP 4 – NFS............................................................................................................................... 24
Configuring the Virtual Service (VIP)............................................................................................................. 24
Defining the Real Servers (RIPs).................................................................................................................. 25
Configuring VIP 5 – ECS Combined Service............................................................................................ 26
Configuring the Virtual Service (VIP)............................................................................................................. 26
Setting Up the TLS/SSL Termination ........................................................................................................... 27
Uploading the Certificate.................................................................................................................................. 27
Creating the TLS/SSL Termination............................................................................................................... 27
Finalizing the Configuration........................................................................................................................ 28

11. Testing & Verification.................................................................................................................................. 28
   Using System Overview.................................................................................................................................. 28

12. Technical Support....................................................................................................................................... 30

13. Further Documentation.............................................................................................................................. 30

14. Conclusion.................................................................................................................................................. 30

15. Appendix.................................................................................................................................................. 31
   1 – Multi-port NFS Health Check................................................................................................................. 31
   2 – Clustered Pair Configuration – Adding a Slave Unit.............................................................................. 32

16. Document Revision History....................................................................................................................... 35
1. About this Guide
This guide details the steps required to configure a load balanced Dell EMC ECS environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Dell EMC ECS 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 Dell EMC ECS. 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>
<tr>
<td></td>
<td>Enterprise GCP **</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

- V8.3.5 and later

4. Dell EMC ECS Software Versions Supported

- Dell EMC ECS – all versions
5. Dell EMC ECS

ECS (Elastic Cloud Storage) is an object storage solution developed by Dell EMC. It uses hardware ‘nodes’ to provide storage, and is designed to be flexible, resilient, and simple to deploy.

Dell recommend the use of load balancing in an ECS deployment, in order to distribute the inbound workload across all ECS nodes in an effort to maximise performance.

One of Dell EMC's approved and documented solutions for load balancing ECS is the free and open source HAProxy load balancer. HAProxy is a key component of the Loadbalancer.org appliance, making it a great fit for load balancing ECS deployments.

6. Load Balancing Dell EMC ECS

Note: It's highly recommended that you have a working Dell EMC ECS environment first before implementing the load balancer.

Persistence (aka Server Affinity)

Persistence is only recommended for NFS connections when load balancing a Dell EMC ECS deployment. This is due to the fact that caching occurs on the ECS servers when the NFS protocol is used. To maximise efficiency, a given NFS client should continue connecting to the same ECS server, so as to continue re-using the established cache.

Virtual Service (VIP) Requirements

To provide load balancing and HA for Dell EMC ECS, the following VIPs are usually required:

- S3 (for object access via the S3 protocol)
- Atmos (for object access via the Atmos protocol)
- Swift (for object access via the Swift protocol)
- NFS (for providing highly available NFS services)

Optionally, additional VIPs may be required as follows:

- ECS Combined Service (for scenario 2, where only a single IP address is client-facing)
- TLS/SSL termination service (for scenario 2, where HTTPS traffic must be decrypted for inspection)

Port Requirements

The following table shows the ports that are load balanced:
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP/HTTP</td>
<td>Object access via HTTP calls</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>Object access via HTTP calls (encrypted HTTPS)</td>
</tr>
<tr>
<td>9020</td>
<td>TCP/HTTP</td>
<td>Object access via the S3 protocol (HTTP)</td>
</tr>
<tr>
<td>9021</td>
<td>TCP/HTTPS</td>
<td>Object access via the S3 protocol (HTTPS)</td>
</tr>
<tr>
<td>9022</td>
<td>TCP/HTTP</td>
<td>Object access via the Atmos protocol (HTTP)</td>
</tr>
<tr>
<td>9023</td>
<td>TCP/HTTPS</td>
<td>Object access via the Atmos protocol (HTTPS)</td>
</tr>
<tr>
<td>9024</td>
<td>TCP/HTTP</td>
<td>Object access via the Swift protocol (HTTP)</td>
</tr>
<tr>
<td>9025</td>
<td>TCP/HTTPS</td>
<td>Object access via the Swift protocol (HTTPS)</td>
</tr>
<tr>
<td>2049</td>
<td>TCP/UDP/NFS</td>
<td>NFS service (mountd and nfsd)</td>
</tr>
<tr>
<td>111</td>
<td>TCP/UDP/ONC RPC</td>
<td>Port mapper service</td>
</tr>
<tr>
<td>10000</td>
<td>TCP/lockd</td>
<td>lockd NFS service</td>
</tr>
</tbody>
</table>

**TLS/SSL Termination**

Terminating TLS/SSL connections on the load balancer is not recommended, due to the significant computational overhead this introduces on the load balancer. Termination and decryption should continue to occur at the ECS servers, which are designed and best placed to perform this function.

It may be necessary to terminate and decrypt traffic at the load balancer, so that it may then be read as plaintext and sorted. This is required if sorting incoming traffic by protocol is not possible by using different ports or IP addresses. This is explained in detail in section 7, *Deployment Concept*.

**Health Checks**

**S3, Atmos, And Swift Virtual Services**

The S3 and Swift virtual services use protocol-specific health checks to query the readiness of a given ECS server to accept connections for those protocols.

The Atmos virtual service uses a standard ‘connect to port’ check, which examines whether the Atmos port is open on a given ECS server to determine whether the server is ready to accept connections using the Atmos protocol.

**NFS Virtual Service**

The NFS virtual service uses a standard ‘connect to port’ check by default, which examines whether the NFS port (2049) is open on a given ECS server to determine whether the server is ready to accept NFS connections.

It is possible to configure a custom health check for the NFS service, which will check the availability of all three ports related to NFS operation (111, 2049, and 10000) on the real servers. Only if all three ports are available will a real server be considered ‘healthy’ and ready to accept NFS connections.

Please see Appendix 1 - *Multi-port NFS Health Check* for instructions on how to configure such a custom health check.
7. Deployment Concept

There are two deployment scenarios when using Loadbalancer.org appliances as part of a Dell EMC ECS deployment.

Scenario 1 – Virtual Services for Each Protocol

VIPs = Virtual IP Addresses

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 section 2 in the appendix on page 32 for more details on configuring a clustered pair.

This is the preferred scenario, and is the easiest to implement. Incoming traffic is not decrypted or modified in any way.

The different protocols are handled by different virtual services on the load balancer. Each virtual service is client-facing. The traffic needs to be sorted by protocol (S3, Atmos, and Swift) by the time it reaches the load balancer, either sorted by port or sorted by IP address. The S3 traffic needs to go to the S3 virtual service, the Atmos traffic needs to go to the Atmos virtual service, and the Swift traffic needs to go to the Swift virtual service.

Method A: Sorting By Port

This is the simplest way of sorting ECS traffic. It assumes that your clients are able to send request traffic using the correct protocol-specific ports. For example, an S3 client would send request traffic using ports 9020 and 9021. This is likely to be the case for an internal, non-public Internet facing ECS deployment.

The load balancer’s S3, Atmos, and Swift virtual services would all use the same IP address, but would each listen on their respective ports in the 9020-9025 range.
Method B: Sorting By IP Address

This sorting method is a good alternative if sorting by port is not a possibility (for example if client traffic is being sent over the public Internet and ports 80 and 443 must be used for all traffic of all protocols).

A simple way of sorting the incoming traffic by protocol is to use multiple DNS records, one for each protocol. For example:

- os.website.org (FQDN for the S3 service) resolves to the IP address of the S3 VIP
- atmos.website.org (FQDN for the Atmos service) resolves to the IP address of the Atmos VIP
- swift.website.org (FQDN for the Swift service) resolves to the IP address of the Swift VIP

If the FQDNs in question need to resolve to public IP addresses, a valid setup would be to put the public IP addresses on an external facing firewall and then forward the traffic to the relevant load balancer VIPs.

Scenario 2 – Single Client-facing Virtual Service

This scenario involves inspecting all incoming HTTP(S) traffic and sorting it by FQDN, so that it may be forwarded to the correct protocol-specific virtual service, i.e. the S3, Atmos, or Swift virtual service.

This deployment type is useful when it is not possible to pre-sort traffic by port (for example if clients are on the public Internet and traffic needs to be sent using ports 80 and 443 only) or by IP address (for example if changing public DNS records is not possible).
The disadvantages of this setup are that it is more complex to set up than scenario 1 and that all incoming TLS/SSL encrypted traffic must be decrypted for inspection, which is CPU intensive on the load balancer.

Helping you Choose the Most Appropriate Deployment Type

1. Can clients send request traffic to the correct protocol-specific ports, i.e. ports 9020-9025 for the S3, Atmos, and Swift protocols?
   - YES: Use Scenario 1, Method A: sorting by port
   - NO: Can the FQDNs for different protocol access be made to resolve to different IP addresses, e.g. atmos.site.org resolves to 64.70.0.1, swift.site.org resolves to 64.70.0.2, etc.?
     - YES: Use Scenario 1, Method B: sorting by IP address
     - NO: Use Scenario 2
8. Loadbalancer.org Appliance – the Basics

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 2 of the appendix on page 32.
9. Appliance Configuration for Dell EMC ECS – Scenario 1

Changing the Global Layer 7 Settings
It is necessary to change some global layer 7 timeout settings when load balancing an ECS deployment.

1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Advanced Configuration
2. Set the Connection Timeout value to 5000
3. Set the Client Timeout value to 50000
4. Set the Real Server Timeout to 50000
5. Click Update to apply the settings

Configuring VIP 1 – S3

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. ECS-S3
3. Set the Virtual Service IP address field as required:
   - If using method A (sorting by port), use the same IP address for all virtual services
   - If using method B (sorting by IP address), use a unique IP address for the S3 virtual service
4. Set the Virtual Service Ports as required:
   - If using method A (sorting by port), use ports 9020,9021
   - If using method B (sorting by IP address), use ports 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 None
9. In the Health Checks section, click Advanced to show more options
10. Set Health Checks to Negotiate HTTP (GET)
11. Set Request to send to /?ping
12. Set Host Header to haproxy
13. 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. Enter an appropriate name for the server in the Label field, e.g. ECS-Node-1
3. Change the Real Server IP Address field to the required IP address, e.g. 192.168.85.50
4. Leave the Real Server Port field blank
5. Click Update
6. Repeat these steps to add additional servers as required

Configuring VIP 2 – Atmos

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. ECS-Atmos
3. Set the Virtual Service IP address field as required:
   - If using method A (sorting by port), use the same IP address for all virtual services
   - If using method B (sorting by IP address), use a unique IP address for the Atmos virtual service
4. Set the Virtual Service Ports as required:
   - If using method A (sorting by port), use ports 9022,9023
• If using method B (sorting by IP address), use ports 80,443
5. Set the Layer 7 Protocol to TCP Mode
6. Click Update to create the virtual service

![Layer 7 - Add a new Virtual Service](image)

7. Click Modify next to the newly created VIP
8. Set Persistence Mode to None
9. 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. Enter an appropriate name for the server in the Label field, e.g. ECS-Node-1
3. Change the Real Server IP Address field to the required IP address, e.g. 192.168.85.50
4. Leave the Real Server Port field blank
5. Click Update
6. Repeat these steps to add additional servers as required

![Layer 7 Add a new Real Server - ECS-Atmos](image)
Configuring VIP 3 – Swift

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. ECS-Swift
3. Set the Virtual Service IP address field as required:
   - If using method A (sorting by port), use the same IP address for all virtual services
   - If using method B (sorting by IP address), use a unique IP address for the Swift virtual service
4. Set the Virtual Service Ports as required:
   - If using method A (sorting by port), use ports 9024,9025
   - If using method B (sorting by IP address), use ports 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 None
9. Set Health Checks to Negotiate HTTP (HEAD)
10. Set Request to send to /healthcheck
11. 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. Enter an appropriate name for the server in the Label field, e.g. ECS-Node-1
3. Change the Real Server IP Address field to the required IP address, e.g. 192.168.85.50
4. Leave the Real Server Port field blank
5. Click **Update**

6. Repeat these steps to add additional servers as required

### Configuring VIP 4 – NFS

**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. **ECS-NFS**

3. Set the *Virtual Service IP address* field to the IP address to be used for NFS access, in this example **192.168.85.200**

4. Set the *Virtual Service Ports* field to **111,2049,10000**

5. Set the *Protocol* to **TCP/UDP**

6. Set the *Forwarding Method* to **SNAT**

7. Click **Update** to create the virtual service
8. Click **Modify** next to the newly created VIP
9. Ensure the **Persistence Enable** checkbox is enabled
10. Set the **Persistence Timeout** field to 86400 (as the units are seconds, this equates to 24 hours)
11. Set **Health Checks** to **Connect to port**
12. Set **Check Port** to **2049**

Note: In the default setup presented here, each ECS server will be checked on port 2049 only (the NFS port) to judge whether the server is ready to accept NFS connections.

It is possible to configure a custom health check for the NFS service, which will check the availability of all three ports related to NFS operation (111, 2049, and 10000) on the real servers. In that case, only if all three ports are available will a real server be considered 'healthy' and ready to accept connections.

Please see Appendix 1 – **Multi-port NFS Health Check** for instructions on how to configure such a custom health check.

13. 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. Enter an appropriate name for the server in the **Label** field, e.g. **ECS-Node-1**
3. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.50**
4. Leave the **Real Server Port** field blank
5. Click **Update**
6. Repeat these steps to add additional servers as required
Finalizing the Configuration

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

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

10. Appliance Configuration for Dell EMC ECS – Scenario 2

Changing the Global Layer 7 Settings

It is necessary to change some global layer 7 timeout settings when load balancing an ECS deployment.

1. Using the web user interface, navigate to **Cluster Configuration > Layer 7 – Advanced Configuration**
2. Set the **Connection Timeout** value to **5000**
3. Set the **Client Timeout** value to **50000**
4. Set the **Real Server Timeout** to **50000**
5. Click **Update** to apply the settings

Configuring VIP 1 – S3

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. **ECS-S3**
3. Set the **Virtual Service IP address** field to an unused IP address, e.g. **192.168.85.200**
4. Set the **Virtual Service Ports** field to **80**
5. Set the **Layer 7 Protocol** to **HTTP Mode**
6. Click **Update** to create the virtual service

![Layer 7 - Add a new Virtual Service](image)

7. Click **Modify** next to the newly created VIP
8. Set **Persistence Mode** to **None**
9. In the **Health Checks** section, click **Advanced** to show more options
10. Set **Health Checks** to **Negotiate HTTP (GET)**
11. Set **Request to send** to **/?ping**
12. Set **Host Header** to **haproxy**
13. 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. Enter an appropriate name for the server in the **Label** field, e.g. **ECS-Node-1**
3. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.50**
4. Set the **Real Server Port** field to **9020**
5. Click **Update**
6. Repeat these steps to add additional servers as required
Configuring VIP 2 – Atmos

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. ECS-Atmos.
3. Set the Virtual Service IP address field to an unused IP address, e.g. 192.168.85.201.
4. Set the Virtual Service Ports field to 80.
5. Set the Layer 7 Protocol to HTTP Mode.
6. Click Update to create the virtual service.

7. Click Modify next to the newly created VIP.
8. Set Persistence Mode to None.
9. 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. Enter an appropriate name for the server in the Label field, e.g. ECS-Node-1.
3. Change the Real Server IP Address field to the required IP address, e.g. 192.168.85.50.
4. Set the Real Server Port field to 9022.
5. Click Update.
6. Repeat these steps to add additional servers as required.
Configuring VIP 3 – Swift

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. ECS-Swift
3. Set the Virtual Service IP address field to an unused IP address, e.g. 192.168.85.202
4. Set the Virtual Service Ports field to 80
5. Set the Layer 7 Protocol to HTTP Mode
6. Click Update to create the virtual service

7. Click Modify next to the newly created VIP
8. Set Persistence Mode to None
9. Set Health Checks to Negotiate HTTP (HEAD)
10. Set Request to send to /healthcheck
11. 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. Enter an appropriate name for the server in the Label field, e.g. ECS-Node-1
3. Change the Real Server IP Address field to the required IP address, e.g. 192.168.85.50
4. Set the Real Server Port field to 9024
5. Click Update
6. Repeat these steps to add additional servers as required
Configuring VIP 4 – NFS

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. ECS-NFS
3. Set the Virtual Service IP address field to the IP address to be used for NFS access, in this example 192.168.85.203
4. Set the Virtual Service Ports field to 111,2049,10000
5. Set the Protocol to TCP/UDP
6. Set the Forwarding Method to SNAT
7. Click Update to create the virtual service
8. Click Modify next to the newly created VIP
9. Ensure the Persistence Enable checkbox is enabled
10. Set the Persistence Timeout field to 86400 (as the units are seconds, this equates to 24 hours)
11. Set Health Checks to Connect to port
12. Set Check Port to 2049

Note: In the default setup presented here, each ECS server will be checked on port 2049 only (the NFS port) to judge whether the server is ready to accept NFS connections.

It is possible to configure a custom health check for the NFS service, which will check the availability of all three ports related to NFS operation (111, 2049, and 10000) on the real servers. In that case, only if all three ports are available will a real server be considered ‘healthy’ and ready to accept connections.

Please see Appendix 1 – Multi-port NFS Health Check for instructions on how to configure such a custom health check.

13. 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. Enter an appropriate name for the server in the Label field, e.g. ECS-Node-1
3. Change the Real Server IP Address field to the required IP address, e.g. 192.168.85.50
4. Leave the Real Server Port field blank
5. Click Update
6. Repeat these steps to add additional servers as required

![Layer 4 Add a new Real Server - ECS-NFS](image-url)
Configuring VIP 5 – ECS Combined Service

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. ECS-Combined-Service
3. Set the Virtual Service IP address field to the IP address that all incoming client traffic will be arriving at on the load balancer. In the example presented here, all client traffic (regardless of port) is being sent to the IP address 192.168.85.150, and so the IP address used for the combined service is 192.168.85.150
4. Set the Virtual Service Ports field to 80
5. Set the Layer 7 Protocol to HTTP Mode
6. Click Update to create the virtual service

<table>
<thead>
<tr>
<th>Label</th>
<th>ECS-Combined-Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.85.150</td>
</tr>
<tr>
<td>Ports</td>
<td>80</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>HTTP Mode</td>
</tr>
<tr>
<td>Manual Configuration</td>
<td></td>
</tr>
</tbody>
</table>

7. Click Modify next to the newly created VIP
8. Under Configure Content Redirects click Edit ACL Rules
9. Create the first ACL rule, which will redirect S3 traffic to the S3 virtual service. Set Rule Type to hdr_host, use the Boolean option Equals, and set the URL Text/IP field to -m dom, to specify domain matching, followed by the domain in question. For example, use -m dom os.website.org (replacing “website.org” with the correct domain, e.g. the domain that clients' S3 protocol traffic is sent to). Note that this rule also picks up traffic to *.os.website.org, which accounts for S3 virtually hosted buckets. Set Rule Action Type to Backend. Finally, set the Redirect Location to the name of the S3 virtual service created earlier, which in the example presented here is ECS-S3. Click the Add button to insert the ACL rule
10. Create similar ACL rules to redirect Atmos and Swift protocol traffic to their respective virtual services in the same way. Use URL Text/IP values of the form atmos.website.org for Atmos traffic and swift.website.org for Swift traffic. The completed set of rules for the example presented here look like the following:
11. Click **Save** to save all of the added ACL rules

12. Click **Update**

**Setting Up the TLS/SSL Termination**

Incoming TLS/SSL encrypted traffic must be decrypted at the load balancer, so that it can then be read as plaintext HTTP traffic. This is necessary to separate the traffic by FQDN using the previously configured ACL rules, i.e. traffic destined for os.website.org (and *.os.website.org) goes to the S3 virtual service, traffic destined for atmos.website.org goes to the Atmos virtual service, and traffic destined for swift.website.org goes to the Swift virtual service.

**Uploading The Certificate**

The appropriate public certificate, including both the private key and public certificate parts, must be uploaded to the load balancer for TLS/SSL termination to work.

Detailed information on creating PEM certificate files and converting between certificate formats is presented in our *Administration Manual*: [http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf](http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf)

The process for uploading a certificate is as follows:

1. Using the web user interface, navigate to Cluster Configuration > SSL Certificate and click on Add a new SSL Certificate
2. Press the Upload prepared PEM/PFX file radio button
3. Define the Label for the certificate as required. It may make sense to use the domain that the certificate is associated to, e.g. website.org
4. Click on Browse and select the appropriate PEM or PFX style certificate
5. If uploading a PFX certificate, enter the certificate’s password in the PFX File Password field
6. Click Upload certificate

**Creating The TLS/SSL Termination**

1. Using the web user interface, navigate to Cluster Configuration > SSL Termination and click on Add a new Virtual Service
2. From the Associated Virtual Service drop-down list, select the ‘ECS Combined’ service that was created
previously, e.g. **ECS-Combined-Service**

3. Set the **Virtual Service Port** field to **443**

4. From the **SSL Certificate** drop-down list, select the certificate for the service in question, which in this example is **website.org**

5. Click **Update** to create the TLS/SSL termination service

---

**Finalizing the Configuration**

To apply the new settings, HAProxy and stunnel must both be reloaded as follows:

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

---

**11. Testing & Verification**

**Using System Overview**

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPS (i.e. the ECS servers) and shows the state/health of each server as well as the state of the cluster as a whole.

The example below shows a **scenario 1** style setup, where all five ECS servers are healthy and available to accept connections for each of the four protocol-specific virtual services:
The example below shows a scenario 2 style setup, where all five ECS servers are healthy and available to accept connections for each of the four protocol-specific virtual services.

Note that the ‘ECS Combined Service’ shows as red, as it does not have any healthy real servers (because it does not have any real servers defined). This is normal, as it is a ‘dummy’ service used only to redirect incoming traffic to the other four virtual services, based on the destination domain of incoming traffic.
12. 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.

13. Further Documentation


14. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Dell EMC ECS environments.
15. Appendix

1 - Multi-port NFS Health Check

A custom health check can be used with the NFS virtual service. This will check the real servers and ensure that all three of the NFS ports (111, 2049, and 10000) are available before considering a server to be online and ready to accept connections.

From an SSH session to the load balancer, or from the console, navigate to the directory /var/lib/loadbalancer.org/check. Open the file Multi-port-check.sh using a text editor (vim and nano are both installed on the appliance).

Change the CHECK_PORT definition so that it reads as:

```
CHECK_PORT="111 2049 10000"
```

Save the modified check file.

Note: If using an HA master-slave pair of load balancers, be sure to make the same change to the Multi-port-check.sh on the slave appliance too.

To put the multi-port check into use, from the WebUI navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Modify next to the NFS virtual service.

Set Health Checks to External script, and then set Check Script to Multi-port-check.sh.

Click Update to apply the change.
2 – 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:

![Create a Clustered Pair](image)

• 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 top of the screen.

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.
## 16. 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>24 December 2018</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>30 August 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.1</td>
<td>13 July 2020</td>
<td>Changed the NFS virtual service to be a layer 4 SNAT mode service</td>
<td>Some NFS applications require UDP traffic, which needs to be handled using a layer 4 service</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added explicit leading forward slashes to the Negotiate HTTP health check 'requests to send'</td>
<td>Reflects a change in the appliance's health check handling</td>
<td></td>
</tr>
<tr>
<td>1.1.2</td>
<td>17 July 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added additional instructions for configuring health checks</td>
<td>Changes to the appliance WebUI</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, BC, V6B 2Z4, Canada
TEL: +1 866 998 0508
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

© Copyright Loadbalancer.org • www.loadbalancer.org