Table of 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 ................................................................ 4
6. Load Balancing Dell EMC ECS .................................................. 4
   Persistence (aka Server Affinity) .................................................. 4
   Virtual Service (VIP) Requirements ............................................. 4
   Port Requirements ................................................................ 5
   TLS/SSL Termination .............................................................. 5
   Health Checks ...................................................................... 5
     S3, Atmos, and Swift Virtual Services ......................................... 5
     NFS Virtual Service ............................................................. 6
7. Deployment Concept ............................................................... 6
   Scenario 1 – Virtual Services for Each Protocol ............................... 6
     Method A: Sorting by Port ..................................................... 7
     Method B: Sorting by IP Address ............................................. 7
   Scenario 2 – Single Client-facing Virtual Service ............................. 7
   Helping you Choose the Most Appropriate Deployment Type ............... 8
8. Loadbalancer.org Appliance – the Basics ......................................... 8
   Virtual Appliance ................................................................ 8
   Initial Network Configuration .................................................... 9
   Accessing the WebUI ................................................................ 9
   Main Menu Options .............................................................. 10
   HA Clustered Pair Configuration ............................................... 11
9. Appliance Configuration for Dell EMC ECS – Scenario 1 ...................... 11
   Changing the Global Layer 7 Settings .......................................... 11
   Configuring VIP 1 – S3 ............................................................ 11
     Configuring the Virtual Service (VIP) ........................................ 11
     Defining the Real Servers (RIPs) ............................................. 12
   Configuring VIP 2 – Atmos ....................................................... 13
     Configuring the Virtual Service (VIP) ........................................ 13
     Defining the Real Servers (RIPs) ............................................. 13
   Configuring VIP 3 – Swift ......................................................... 14
     Configuring the Virtual Service (VIP) ........................................ 14
     Defining the Real Servers (RIPs) ............................................. 15
   Configuring VIP 4 – NFS .......................................................... 15
     Configuring the Virtual Service (VIP) ........................................ 15
     Defining the Real Servers (RIPs) ............................................. 16
   Finalizing the Configuration ..................................................... 17
10. Appliance Configuration for Dell EMC ECS – Scenario 2 .................. 17
    Changing the Global Layer 7 Settings .......................................... 17
    Configuring VIP 1 – S3 ............................................................ 17
      Configuring the Virtual Service (VIP) ........................................ 17
      Defining the Real Servers (RIPs) ............................................. 18
    Configuring VIP 2 – Atmos ....................................................... 19
      Configuring the Virtual Service (VIP) ........................................ 19
      Defining the Real Servers (RIPs) ............................................. 19
    Configuring VIP 3 – Swift .......................................................... 20
Configuring the Virtual Service (VIP) .................................................. 20
Defining the Real Servers (RIPs) .................................................. 21
Configuring VIP 4 – NFS ................................................................. 21
  Configuring the Virtual Service (VIP) ........................................... 21
  Defining the Real Servers (RIPs) .................................................. 22
Configuring VIP 5 – ECS Combined Service .................................. 23
  Configuring the Virtual Service (VIP) ........................................... 23
Setting Up the TLS/SSL Termination ................................................ 24
  Uploading the Certificate ............................................................. 24
  Creating the TLS/SSL Termination ............................................. 25
Finalizing the Configuration ........................................................... 25
11. Testing & Verification ................................................................. 25
  Using System Overview ............................................................... 25
12. Technical Support ................................................................. 27
13. Further Documentation .............................................................. 27
14. Conclusion .............................................................................. 27
15. Appendix .............................................................................. 28
  Multi-port NFS Health Check ...................................................... 28
  Configuring HA - Adding a Secondary Appliance ....................... 28
16. Document Revision History .......................................................... 31
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 Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Dell EMC ECS. For full specifications of available models please
refer to https://www.loadbalancer.org/products. Some features may not be supported in all cloud platforms due to
platform specific limitations, please check with Loadbalancer.org support for further details.

3. Loadbalancer.org Software Versions Supported

- V8.3.8 and later

4. 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 maximize 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 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 refer to the Appendix section 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

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

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

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

8. Loadbalancer.org Appliance – the Basics

Virtual Appliance
A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.
The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance’s WebUI.

Note

Please refer to The Virtual Appliance - Hypervisor Deployment and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Note

For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.

Initial Network Configuration

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

Important

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

Accessing the WebUI

The WebUI is accessed using a web browser. By default, user authentication is based on local Apache .htaccess files. User administration tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.

Note

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

Note

If required, users can also be authenticated against LDAP, LDAPS, Active Directory or Radius. For more information please refer to External Authentication.

1. Using a browser, access the WebUI using the following URL:


2. Log in to the WebUI:

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

   Note

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

Once logged in, the WebUI will be displayed as shown below:
Note: The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.

3. You'll be asked if you want to run the Setup Wizard. If you click **Accept** the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simple click **Dismiss**.

**Main Menu Options**

- **System Overview** - Displays a graphical summary of all VIPs, RIPS and key appliance statistics
- **Local Configuration** - Configure local host settings such as IP address, DNS, system time etc.
- **Cluster Configuration** - Configure load balanced services such as VIPs & RIPS
- **Maintenance** - Perform maintenance tasks such as service restarts and taking backups
- **View Configuration** - Display the saved appliance configuration settings
- **Reports** - View various appliance reports & graphs
HA Clustered Pair Configuration
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in appendix section Configuring HA - Adding a Secondary Appliance.

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.

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.
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.

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 refer to the appendix section **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.
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.

![Layer 7 Add a new Real Server - ECS-Swift](image)

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 refer to the appendix section **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.
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.

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:

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>Boolean</th>
<th>URL Text/IP</th>
<th>Rule Action Type</th>
<th>Redirect Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Equals</td>
<td>-m dom os.website.org</td>
<td>Drop</td>
<td></td>
</tr>
<tr>
<td>hdr_host</td>
<td>Equals</td>
<td>-m dom os.website.org</td>
<td>Backend</td>
<td>ECS-S3</td>
</tr>
<tr>
<td>hdr_host</td>
<td>Equals</td>
<td>-m dom swift.website</td>
<td>Backend</td>
<td>ECS-Swift</td>
</tr>
<tr>
<td>hdr_host</td>
<td>Equals</td>
<td>-m dom atmos.website</td>
<td>Backend</td>
<td>ECS-Atmos</td>
</tr>
</tbody>
</table>

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.

For more information on creating PEM certificate files and converting between certificate formats please refer to Creating a PEM File

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.

![SSL Termination - Add a new Virtual Service](image)

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

   Note  For additional general guidance please also refer to Testing Load Balanced Services.

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

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.

1. From an SSH session to the load balancer, or from the console, navigate to the directory `/var/lib/loadbalancer.org/check`.

2. Open the file Multi-port-check.sh using a text editor (vim and nano are both installed on the appliance).

3. Change the CHECK_PORT definition so that it reads:

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

4. Save the modified check file.

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

5. 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.

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

7. Click Update to apply the change.

Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution.

We recommend that the Primary appliance should be configured first, then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically replicated to the Secondary over the network using SSH/SCP.

**Note** For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified – one for the VIP when it’s active on the Primary and one for the VIP when it’s active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

**Note** A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:
<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface Configuration</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced Configuration</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>

To add a Secondary node - i.e. create a highly available clustered pair:

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

![CREATE A CLUSTERED PAIR](loadbalancer.org)

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

![CREATE A CLUSTERED PAIR](image)

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

![High Availability Configuration - primary](image)

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

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

**Note**
For more details on configuring HA with 2 appliances, please refer to [Appliance Clustering for HA](#).
## 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>
<tr>
<td>1.2.0</td>
<td>1 November 2021</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</td>
</tr>
</tbody>
</table>
About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.