# Table of Contents

1. About this Guide .......................................................... 3
2. Loadbalancer.org Appliances Supported .................................. 3
3. Loadbalancer.org Software Versions Supported .......................... 3
4. IBM Cloud Object Storage Software Versions Supported ............... 3
5. Load Balancing IBM Cloud Object Storage Accessor Nodes ............. 3
   Application Prerequisites ................................................. 4
   Port Requirements ....................................................... 4
   Deployment Concept .................................................... 4
   - HTTP and HTTPS (SSL Pass-through) load balancing ............ 4
   - HTTP and HTTPS (SSL Termination) load balancing .......... 5
   Virtual Service (VIP) Requirements .................................... 5
   Deployment Mode ....................................................... 5
6. Loadbalancer.org Appliance – the Basics .................................. 5
   Virtual Appliance ....................................................... 5
   Initial Network Configuration .......................................... 6
   Accessing the WebUI .................................................... 6
   - Main Menu Options .................................................. 7
   HA Clustered Pair Configuration ....................................... 8
7. Appliance & IBM Accessor Node Configuration .......................... 8
   Appliance Configuration ............................................... 8
   - Configuring VIP1 – Accessor Cluster using SSL Pass-through ...... 8
   - Configuring VIP1 – Accessor Cluster using SSL Termination ...... 9
8. Additional Configuration Options & Settings ............................ 10
   SSL Termination ....................................................... 10
   - SSL Termination on the load balancer - SSL Offloading ............ 11
   - Certificates .......................................................... 11
   - Configuring SSL Termination on the Load Balancer .............. 13
   - Finalizing the Configuration ........................................ 14
9. Testing & Verification ...................................................... 14
   - Using System Overview ............................................. 14
10. Technical Support ......................................................... 14
11. Further Documentation ................................................... 14
12. Conclusion ........................................................................ 14
13. Appendix .......................................................................... 16
   - Configuring GSLB / Location Affinity ............................... 16
   - Conceptual Overview ................................................ 16
   - Appliance Configuration ............................................. 17
   - DNS Server Configuration .......................................... 19
   Alternative Load Balancing Method for Read-Intensive Deployments (Direct Routing) .... 19
   - Caveats .................................................................. 20
   - Appliance Configuration for IBM COS Accessor Nodes – Using Layer 4 DR Mode (Direct Routing) .................. 20
   - Configuring HA - Adding a Secondary Appliance ............... 21
14. Document Revision History ................................................ 24
1. About this Guide

This guide details the steps required to configure a highly available IBM Cloud Object Storage Accessor node environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Accessor node configuration changes that are required.

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 IBM Cloud Object Storage. 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

- V8.4.1 & later

4. IBM Cloud Object Storage Software Versions Supported

- IBM Cloud Object Storage – all versions

5. Load Balancing IBM Cloud Object Storage Accessor Nodes

The IBM COS system is a breakthrough cloud platform that helps solve petabyte and beyond storage challenges for enterprises worldwide. It uses an innovative and cost-effective approach for storing large volumes of unstructured data while still ensuring scalability, security, availability, reliability, manageability, and flexibility.

- Scalability offers a single storage system and namespace versus an ever-increasing number of limited-capacity storage silos
- Security features include a wide range of capabilities designed to help meet security requirements
- Availability and reliability characteristics of the system are configurable to best suit different use cases and requirements
- Manageability helps enable storage administrators to handle large storage capacity
- Flexibility of a software-defined storage solution that does not require specific or proprietary hardware

For high availability and scalability, IBM recommend that a load balancer is used to distribute client connections to the IBM Accessor node clusters. Load balancers monitor and perform health checks on a node to ensure traffic is routed correctly to healthy nodes. Without the use of a load balancer, an offline or failed node would still receive traffic, causing failures.

A variety of load balancing methods are currently supported by IBM COS Accessor nodes, dependent on customer infrastructure, including layer 4, layer 7, and geo GSLB / location affinity.

Application Prerequisites

Network Time Protocol (NTP) configuration is required for proper operations of an IBM COS system. Time must be synchronized not only among the IBM COS nodes but also across all connecting clients. Typically, the IBM COS manager node synchronizes with an external time source, and all other nodes synchronize with the manager node.

© Copyright Loadbalancer.org • Documentation • Load Balancing IBM Cloud Object Storage
It is therefore advised to configure the NTP settings on the load balancer which can be found via the WebUI under *Local Configuration > System Date & Time*.

### System Date & Time

- **Current system time**: 2020-03-17 16:09:25 UTC
- **System Timezone**: UTC
- **NTP Servers**:

### Port Requirements

The following table shows the ports used by the IBM Accessor nodes. The load balancer must be configured to listen on the same ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/8080</td>
<td>TCP/HTTP</td>
<td>HTTP &amp; Object Interfaces to Vaults</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>HTTPS for dsNet Auth/Registry Data</td>
</tr>
</tbody>
</table>

### Deployment Concept

When the IBM Accessor nodes are deployed with the load balancer, clients connect to the Virtual Service (VIP) on the load balancer rather than connecting directly to one of the Accessor nodes.

**HTTP and HTTPS (SSL Pass-through) load balancing**
HTTP and HTTPs (SSL Termination) load balancing

Note

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

Virtual Service (VIP) Requirements

To provide load balancing for IBM COS Accessor nodes the following VIP is required:

- **VIP 1**: Accessor Cluster

Deployment Mode

As mentioned above, the VIP can be configured using either Layer 4 or Layer 7, depending on the architecture of the network. In this case we recommend using Layer 7 as no network changes are required and SSL termination can be implemented. This mode offers high performance and implementation flexibility, however as Layer 7 is a reverse proxy the client source IP address is not visible at the real server: instead, the IP address of the load balancer is visible at the real server. In order to retain the client source IP address, the load balancer inserts an X-Forwarded-For header into the load balanced traffic, which the IBM Accessor nodes can log for troubleshooting issues while seeing the true source IP address of connecting clients.

6. 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.

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.
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.

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, RIPv 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 & RIPv
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 Configuring HA - Adding a Secondary Appliance.

7. Appliance & IBM Accessor Node Configuration

Appliance Configuration
Configuring VIP1 – Accessor Cluster using SSL Pass-through
a) Setting up the Virtual Service (VIP)
1. Using the WebUI, navigate to Cluster Configuration > Layer 7 – Virtual Services and click Add a new Virtual Service.
2. Enter the following details:

   **Layer 7 - Add a new Virtual Service**

<table>
<thead>
<tr>
<th>Manual Configuration</th>
<th>Label</th>
<th>IP Address</th>
<th>Ports</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Accessor Cluster</td>
<td>192.168.0.200</td>
<td>443</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

   3. Enter an appropriate label (name) for the VIP, e.g. Accessor Cluster.
   4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.0.200.
   5. Set the Virtual Service Ports field to 443.
   6. Leave Protocol set to TCP.
   7. Click Update.
   8. Click Modify next to the newly created VIP.
   9. Set Persistence Mode to None.
   10. Set Health Checks to Connect to Port.
   11. Click Update.
b) Setting up the Real Servers (RIPs)
1. Using the WebUI, navigate to Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created Accessor Cluster VIP.

2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>Accessor node 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.0.41</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label (name) for the RIP, e.g. Accessor node 1.
4. Set the Real Server IP Address field to the IP address of the Accessor node 1.
5. Click Update.
6. Repeat these steps to add additional Accessor nodes as real servers as required.

Configuring VIP1 – Accessor Cluster using SSL Termination

a) Setting up the Virtual Service (VIP)
1. Using the WebUI, navigate to Cluster Configuration > Layer 7 – Virtual Services and click Add a new Virtual Service.

2. Enter the following details:

<table>
<thead>
<tr>
<th>Virtual Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Configuration</td>
</tr>
<tr>
<td>Label</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Ports</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label (name) for the VIP, e.g. Accessor Cluster.
4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.0.150.

5. Set the Virtual Service Ports field to 80 or 8080.

6. Leave Protocol set to HTTP.

7. Click Update.

8. Click Modify next to the newly created VIP.

9. Set Persistence Mode to None.

10. Set Health Checks to Connect to Port.

11. Click Update.

Note: When configuring a layer 7 HTTP mode virtual service the X-Forward-For header is automatically enabled within the Other > Advanced > Set X-Forward-For header to assist in retaining the visibility of the client source IP at the real server.

b) Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created Accessor Cluster VIP.

2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>Accessor node 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.0.41</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label (name) for the RIP, e.g. Accessor node 1.

4. Set the Real Server IP Address field to the IP address of the Accessor node 1.

5. Click Update.

6. Repeat these steps to add additional Accessor nodes as real servers as required.

8. Additional Configuration Options & Settings

SSL Termination

SSL termination can be handled in the following ways:

1. On the Real Servers - aka SSL Pass-through

2. On the load balancer – aka SSL Offloading (recommend for IBM COS Accessor Nodes)
3. On the load balancer with re-encryption to the backend servers – aka **SSL Bridging**

In the case of IBM COS Accessor Nodes, it is recommended that SSL be terminated on the load balancer (**SSL offloading**) with **Force to HTTPS** enabled.

SSL termination on the load balancer can be very CPU intensive.

By default, a self-signed certificate is used for the new SSL VIP. Certificates can be requested on the load balancer or uploaded as described in the section below. The default self-signed certificate can be regenerated if needed using the WebUI menu option: SSL Certificate and clicking the **Regenerate Local SSL Certificate** button.

The backend for the SSL VIP can be either a Layer 7 SNAT mode VIP or a Layer 4 NAT or SNAT mode VIP. Layer 4 DR mode cannot be used since stunnel acts as a proxy, and the Accessor node servers see requests with a source IP address of the VIP. However, since the Accessor node servers believe that they own the VIP (due to the loopback adapter configured to handle to ARP problem) they are unable to reply to stunnel.

### SSL Termination on the load balancer - SSL Offloading

In this case, an SSL VIP utilizing stunnel is configured on the appliance and an SSL certificate is uploaded and associated to the Virtual Service. Data is encrypted from the client to the load balancer, but is un-encrypted from the load balancer to the backend servers as shown above.

### Certificates

If you already have an SSL certificate in either PFX or PEM file format, this can be uploaded to the Load balancer using the certificate upload option as explained in **Uploading Certificates**. Alternatively, you can create a Certificate Signing Request (CSR) and send this to your CA to create a new certificate.

**Generating a CSR on the Load Balancer**

CSR’s can be generated on the load balancer to apply for a certificate from your chosen CA.
To generate a CSR:

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificates*.

2. Click **Add a new SSL Certificate** & select **Create a New SSL Certificate (CSR)**.

3. Enter a suitable label (name) for the certificate, e.g. *Cert1*.

4. Populate the remaining fields according to your requirements.

5. Once all fields are complete click **Create CSR**.

6. To view the CSR click **Modify** next to the new certificate, then expand the Certificate Signing Request (CSR) section.

7. Copy the CSR and send this to your chosen CA.

8. Once received, copy/paste your signed certificate into the Your Certificate section.

9. Intermediate and root certificates can be copied/pasted into the Intermediate Certificate and Root Certificate sections as required.

10. Click **Update** to complete the process.

**Uploading Certificates**

If you already have a certificate in either PEM or PFX format, this can be uploaded to the load balancer.

To upload a Certificate:

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificates*.

2. Click **Add a new SSL Certificate** & select **Upload prepared PEM/PFX file**.
3. Enter a suitable Label (name) for the certificate, e.g. **Cert1**.

4. Browse to and select the certificate file to upload (PEM or PFX format).

5. Enter the password, if applicable.

6. Click **Upload Certificate**, if successful, a message similar to the following will be displayed:

   ![Certificate Upload Success Message]

   **Information:** cert1 SSL Certificate uploaded successfully.

   **Note** It’s important to backup all of your certificates. This can be done via the WebUI from **Maintenance > Backup & Restore > Download SSL Certificates**.

### Configuring SSL Termination on the Load Balancer

**To configure an SSL VIP:**

1. Using the WebUI, navigate to **Cluster Configuration > SSL Termination** and click **Add a new Virtual Service**.

   ![SSL Termination Add Virtual Service]

   **Label**
   
   **Associated Virtual Service**
   
   **Virtual Service Port**
   
   **SSL Operation Mode**
   
   **SSL Certificate**

   2. Set **Associated Virtual Service** to the appropriate VIP, e.g. **Accessor_Cluster**. This will automatically fill in the label as the VIP name with SSL inserted in front of the VIP name e.g. **SSL-Accessor_Cluster**.

   **Note** The Associated Virtual Service drop-down is populated with all single port, standard (i.e. non-manual) Layer 7 VIPs available on the load balancer. Using a Layer 7 VIP for the backend is the recommended method although as mentioned earlier, Layer 4 NAT mode and layer 4 SNAT mode VIPs can also be used if required. To forward traffic from the SSL VIP to these type of VIPs, you’ll need to set Associated Virtual Service to **Custom**, then configure the IP address & port of the required VIP.
3. Leave Virtual Service Port set to 443.
5. Select the required certificate from the SSL Certificate drop-down.
6. Click Update.
7. Click Reload STunnel when prompted to apply the new settings using the button provided in the blue box.

Once configured, HTTP traffic will be load balanced by the Layer 7 SNAT mode VIP and HTTPS traffic will be terminated by the SSL VIP, then passed on to the Layer 7 SNAT mode VIP as unencrypted HTTP for load balancing.

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.

9. 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 Accessor Nodes) and shows the state/health of each server as well as the state of the each cluster as a whole. The example below shows that all Accessor nodes are healthy and available to accept connections.

![System Overview](image)

10. 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.

11. Further Documentation

12. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced IBM Cloud
Object Storage environments.
13. Appendix

Configuring GSLB / Location Affinity

Conceptual Overview
For multi-site IBM COS deployments, it is possible to use the load balancer’s GSLB functionality to provide high availability and location affinity across multiple sites.

- Clients across multiple sites can use the same fully qualified domain name to access Accessor nodes
- Under normal operation, clients are directed to their site’s local Accessor node cluster
- In the event that a site’s Accessor node cluster and/or load balancers are off-line then local clients are automatically directed to a functioning Accessor node cluster at another site

For the sake of simplicity, the diagram presented below shows a two site setup. The principle can be extended to encompass as many sites as desired.

Explanation:
- **Start**: A client tries to access the IBM COS Accessor node cluster by using the service’s fully qualified domain name, in this example `ibmcos-region1.domain.tld`
- The client sends a DNS query for `ibmcos-region1.domain.tld` to its local DNS server
The local site’s DNS server has the domain `ibmcos-region1.domain.tld` delegated to the load balancers.

The DNS server sends a delegated DNS query for `ibmcos-region1.domain.tld` to one of the load balancers.

The load balancer that received the delegated DNS query replies to the DNS server by serving up the appropriate local VIP address. For example, if the query originated from the 10.0.0.0/24 subnet, then the VIP in that subnet is served up. Likewise, if the query originated from the 172.16.0.0/24 subnet then the VIP in that subnet is served up. As such, clients are always directed to their local, on-site Accessor node instance, provided that the on-site instance is online and available.

The DNS server sends the delegated DNS answer to the client.

Finish: The client connects to the Accessor node cluster at `ibmcos-region1.domain.tld` by using the local VIP address.

**Note**

In the event that the Accessor node cluster and/or load balancers at one site should completely fail then local clients will be directed to the Accessor node cluster at the other site and the service will continue to be available.

Handling Multiple Sub domains

In some cases IBM COS Accessor node DNS configurations may require the use of multiple DNS sub domains (for example):

- `ibmcos-<region/location>.domain.tld` (e.g. `ibmcos-region1.domain.tld`)

Due to the complexity of DNS delegation, it is recommended to delegate a single sub domain using the GSLB service and then using CNAME records to point everything else at the delegated sub domain. This makes it much easier to configure many DNS entries, including more complex options such as using wildcard entries, for example `*.ibmcos-region1.domain.tld`.

Appliance Configuration

The GSLB service must be configured on the Primary load balancer appliance at each site. The GSLB configuration must be identical across all sites. Configuration takes place in two locations in the WebUI:

- Polaris config: the main configuration for the Polaris service which handles GSLB
- Topology config: defines the network topology, mapping network subnets to sites

Polaris Config

Using the web user interface of the Primary appliance, navigate to **Cluster Configuration > GSLB Configuration** and select **Polaris Config** from the drop-down list.

If GSLB has never been configured then the default example configuration will be displayed in the text box.

What follows is an IBM COS specific example configuration which covers three example sites. It can be copied and pasted to replace the default example and can be used as a basis for creating a deployment-specific configuration.

The elements presented in **boldface** should be customized to reflect the Accessor node deployment in question.
Stanzas should be added or removed under the ‘members’ section as needed to reflect all sites that are to be used in the deployment.

Be sure to click the **Update** button when finished to write the configuration to disk.

**Note**

Indentation is important and **must** be preserved, otherwise the underlying Polaris service will throw an error. As many PDF readers discard leading whitespace, a configuration example can also be found at the following location as a plain text file, in an effort to preserve the indentation when copying: **Load balancer WebUI > Cluster Configuration > GSLB > Polaris Config.**

```plaintext
globalnames:
  ibmcos-region1.domain.tld:
    pool: Accessor-nodes
    ttl: 5

pools:
  Accessor-nodes:
    monitor: http
    monitor_params:
      use_ssl: true
      hostname: ibmcos-region1.domain.tld
      url_path: /
    lb_method: twrr
    fallback: any
    members:
    - ip: 10.0.0.2
      name: node1-dc1
      weight: 1
    - ip: 172.16.0.2
      name: node2-dc2
      weight: 1
    - ip: 192.168.1.2
      name: node3-dc3
      weight: 1
```

**Topology Config**

Using the web user interface of the Primary appliance, navigate to **Cluster Configuration > GSLB Configuration** and select **Topology Config** from the drop-down list.

If GSLB has never been configured then the default example topology configuration will be displayed in the text box.

What follows is a IBM COS specific example topology configuration which covers the same three example sites from the example configuration in the previous section. It can be copy and pasted to replace the default topology example and can be used as a basis for creating a deployment-specific configuration.

The titles and IP subnets should be customised to reflect the IBM COS Accessor node deployment in question. Stanzas should be added or removed as needed to reflect all sites that are to be used in the deployment.

Be sure to click the **Update** button when finished to write the configuration to disk.

```plaintext
datacenter1:
  - 10.0.0.0/24

datacenter2:
  - 172.16.0.0/24

datacenter3:
  - 192.168.0.0/18
```
Applying the Configuration

If updating the configuration of an existing GSLB configuration then press the Reload GSLB button when prompted.

If setting up the GSLB service for the first time then the service must undergo a full restart to be enabled and for the configuration to be applied. To do this, using the web user interface, navigate to Maintenance > Restart Services and click the Restart GSLB button. If using an HA pair of load balancers at a site then this procedure must also be carried out on the Secondary appliance. Once this procedure been carried out it never needs to be done again; the GSLB service only needs to be reloaded in the future when prompted, for example following a configuration change, something that only needs to be carried out on the Primary appliance.

DNS Server Configuration

Once the GSLB service has been configured on the Primary load balancer at every site, ensuring that the configuration is identical across all sites, the DNS server at each site must then be configured for GSLB.

The DNS server at each site must be configured to delegate DNS requests for the subdomain in question to the load balancers; the load balancers' GSLB services will serve the appropriate IP addresses to the DNS servers. Using the example presented throughout this appendix, the DNS server at each site would be configured with a delegation for the domain ibmcos-region1domainтол. The domain would be delegated to every load balancer across every site, which provides multi-site redundancy.

The exact steps for creating a DNS delegation vary between different DNS servers and are outside the scope of this document. For further information, a blog post that walks through creating a DNS delegation on a Microsoft DNS server in the context of setting up GSLB on our appliance can be found at https://www.loadbalancer.org/blog/loadbalancer-org-releases-a-gslb/ (see the section titled “Delegating your subdomain to your GSLB’s using Microsoft’s DNS Server”).

Alternative Load Balancing Method for Read-Intensive Deployments (Direct Routing)

Direct routing, also known as direct server return or DSR, is a method of load balancing. With direct routing, reply traffic flows directly from the back end servers to the clients. In this way, the load balancer is completely bypassed on the return journey for a given connection, thus removing the load balancer as a potential bottleneck for traffic on the return path.

This alternative method of load balancing can benefit read-intensive deployments which feature a large reply traffic to request traffic ratio. For example, consider the scenario where a typical client request is 10 kB in size while a typical reply is 10 GB in size (perhaps file retrieval or video streaming). Direct routing benefits such scenarios: the much larger volume of reply traffic bypasses the load balancer and is not limited by the load balancer’s network throughput. The reply traffic is instead limited by the total available network bandwidth between the servers and the clients, which is limited only by the underlying infrastructure.
Caveats

There are caveats for using the direct routing load balancing method which should be considered:

- The load balancers must be on the same network segment / switching fabric as the Accessor nodes (due to the fact that this load balancing method works by rewriting MAC addresses, i.e. operates at layer 2 of the OSI model).
- Each Accessor node must own the VIP address so that they can all accept and reply to the load balanced traffic. This address should be assigned to a loopback network adaptor.
- Each Accessor node must be configured to not reply to ARP requests for the VIP address or advertise that they own the address.

For guidance on configuring the Accessor nodes for direct routing, in the context of the caveats described above, please consult with the IBM COS team or Support.

Appliance Configuration for IBM COS Accessor Nodes – Using Layer 4 DR Mode (Direct Routing)

Configuring VIP 1 – Accessor Cluster

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. Accessor Cluster.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.0.167.
4. Set the Ports field to 80.
5. Leave the Protocol set to TCP.
7. Click Update to create the virtual service.
8. Click Modify next to the newly created VIP.
9. Ensure that the Persistence Enable checkbox is unchecked.
10. Set the Health Checks Check Type to Connect to port.
11. Set the Check Port to 80.
12. Click Update.

Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Real Servers and click on Add a new Real Server next to the newly created VIP.
2. Define the Label for the real server as required, e.g. accessor-node1.
3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.0.41.
4. Click Update.
5. Repeat these steps to add additional Accessor nodes as real servers as required.

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.

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.

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</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</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.
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](#).
## 14. 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>19 March 2020</td>
<td>Initial version</td>
<td></td>
<td>IBG</td>
</tr>
<tr>
<td>1.0.1</td>
<td>2 September 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>1.1.0</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.