



SOFTWARE VERSION
3.0

EdgeGSLB

Administrator User Guide

Document Properties

Document Number: 2.0.9.26.25.11.09

Document Creation Date: 11 February 2025

Document Last Edited: 26 September 2025

Document Author: Jay Savoor

Document Last Edited by:

Document Disclaimer

This manual's screenshots and graphics may differ slightly from your product due to differences in product release. Edgenexus ensures that they make every reasonable effort to ensure that the information in this document is complete and accurate. Edgenexus makes changes and corrections to the information in this document in future releases when the need arises. Edgenexus assumes no liability for any errors.

Copyrights

© 2025 All rights reserved.

Information in this document is subject to change without prior notice and does not represent a commitment on the manufacturer's part. No part of this guide may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of the manufacturer. Registered trademarks are properties of their respective owners. Every effort is made to make this guide as complete and accurate as possible, but no warranty of fitness is implied. The authors and the publisher shall have neither responsibility nor liability to any person or entity for loss or damages arising from using the information contained in this guide.

Trademarks

Edgenexus logo, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS are all Edgenexus Limited's trademarks. All other trademarks are the properties of their respective owners and are acknowledged.

Edgenexus Support

If you have any technical questions regarding this product, please raise a support ticket at:
support@edgenexus.io

Table of Contents

Document Properties	1
Document Disclaimer	1
Copyrights	1
Trademarks	1
Edgenexus Support	1
GSLB Explained	5
EdgeGSLB – The mechanics	5
Geographical Active-Active	5
Effective Disaster Recovery (DR)	6
Zero-Touch Scalability	6
Installing the EdgeGSLB App	7
Getting the EdgeGSLB from the App Store	7
Downloading and importing the App using the EdgeADC	9
Download and import the App using direct download	9
Making the EdgeGSB App operational	10
Configuring the EdgeGSLB	12
Example network	12
Configuring your EdgeGSLB	12
Adding a new zone (aka domain)	13
Configuring the Associated Virtual Services	15
GSLB Virtual Services	17
GSLB Policies	17
Custom Locations	19
How the Custom Locations feature works	19
Adding A Records for the custom locations	20
Traffic Flow	21
Primary-Secondary DNS Replication	22
How It Works	22
Primary GSLB Configuration	22
Secondary GSLB Configuration	22
AXFR Transfer Process	22
Failover & Load Distribution	22
Key Benefits	22
Setting up the Primary and Secondary(s)	22
Configuring for DNS Replication	23

Dual Data Centre – Dual Arm Example	25
Zone Settings	26
Allow PTR Creation.....	26
DynDNS 2 Settings	26
Zone Access Control.....	26
Change Zone Type	27
Change SOA-EDIT-API.....	27
Remove Zone	28
Administration.....	29
Users.....	30
Creating a User.....	30
Activity.....	32
Server Statistics.....	33
Description in brief	33
General Metrics	33
Query Handling	33
Response Handling	33
Cache Performance.....	34
Backend & Database.....	34
Example Scenarios	34
Scenario 1: High Query Latency (Slow DNS Responses).....	34
Scenario 2: High Backend Load	35
Scenario 3: Frequent DNS Failures (SERVFAIL).....	35
Scenario 4: High NXDOMAIN Responses (Non-Existent Domains).....	35
Scenario 5: High Number of Dropped Queries.....	35
Scenario 6: Poor Cache Performance	36
Scenario 7: High Volume of Corrupt Packets.....	36
Scenario 8: High Number of DNSSEC Queries	36
Zone Templates.....	37
Key Features of Zone Templates	37
Usage Workflow.....	37
Modify and Manage Templates	37
Settings	38
AXFR Settings.....	39
Overview of AXFR in EdgeGSLB	39
How AXFR Works in EdgeGSLB.....	39
Global Settings	41

What is Proxy Protocol?	41
Server Settings	42
Logging and Log Levels	42
Zone Settings	44

GSLB Explained

GSLB, or its full name Global Server Load Balancing, allows organizations to improve their IT resilience using multiple data centres, on-ground or in-cloud. EdgeGSLB works by using server health and DNS to direct the traffic across geographical sets based on logic defined by the networking administrator.

The great thing about EdgeGSLB is that its resilience is no-touch, meaning that failover, fallback, or redirection of traffic is seamless should any resources within a data centre fail.

EdgeGSLB can also drive traffic based on geo-proximity, so users can obtain the lowest possible latency when accessing the applications within the data centre. Geo-proximity means that Melbourne users are sent to an Australian data centre, while users in Frankfurt can be sent to their nearest location, London. If the Australian data centre fails, its users will automatically be diverted to the London data centre until fixes are made.

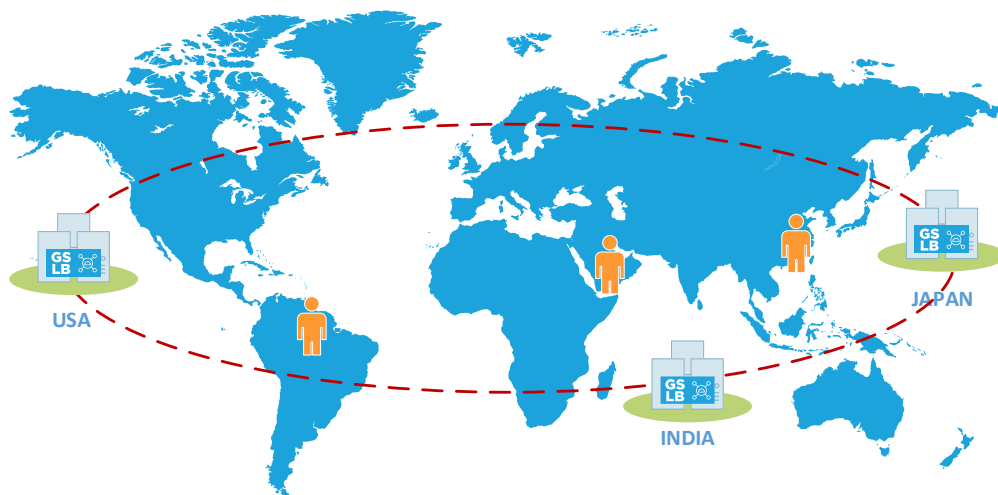
The advantage of using the EdgeGSLB is that it is totally under your control and does not rely on external DNS or other contractual services.

EdgeGSLB – The mechanics

There are some use cases for EdgeGSLB, and in this document, we will work to explain these to you.

Geographical Active-Active

This illustration is the classic way in which most organizations use EdgeGSLB. It operates by forming an Active-Active high availability framework of data centre server farms. Users can be located across geographies, and their requests are sent to the nearest and available data centre to have the best user experience.



End users from across the globe will access their application, with the EdgeGSLB determining where best to route the requests. The 'where best' is decided by the EdgeGSLB based on the system administrator's specified geo-proximity configuration.

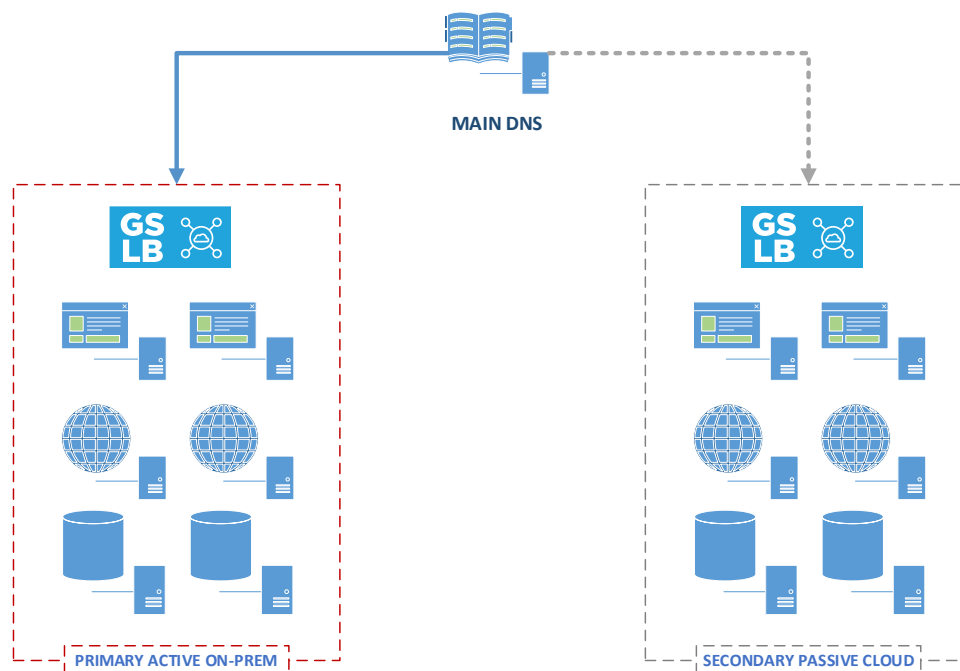
The health of each server within each data centre is continually monitored using various monitoring methods available. If an anomaly is detected within any data centre, the EdgeGSLB in that location will automatically route the end user to one of the other available and working server farms. We call this an Active-Active configuration because all the EdgeGSLB modules, servers, and data centres are accessible and operational.

Effective Disaster Recovery (DR)

The Edgenexus GSLB solution can be deployed to form a highly effective disaster recovery solution.

In standard DR scenarios, failure of the primary site would mean that the DNS entries would need to be manually changed to point to the secondary DR location and then back again when failback is initiated.

In the case of a data centre or services failure in the primary location, the EdgeGSLB will initiate a failover to the secondary. Using Edgenexus GSLB, this is no longer required. The image below shows two data centre locations, with an ADC+EdgeGSLB in each and a continual health check on their respective server farms.



Should the EdgeGSLB instances determine that the health of the primary data centre or any of its applications poses a problem, the failover to the secondary will be initiated.

Zero-Touch Scalability

Another good use case of the EdgeGSLB is 'zero-touch scalability'.

Let us look at a scenario with a primary data centre on-premise. We currently have several application servers in a cloud data centre, and we use GSLB for high availability. We then experience a sudden upsurge in usage and risk our servers being stressed.

The EdgeGSLB can monitor the usage in the primary on-premise servers and redirect users to the secondary cloud-located servers when needed. Since cloud data centres can utilize elastic computing, this method proves to be highly cost-effective to use.

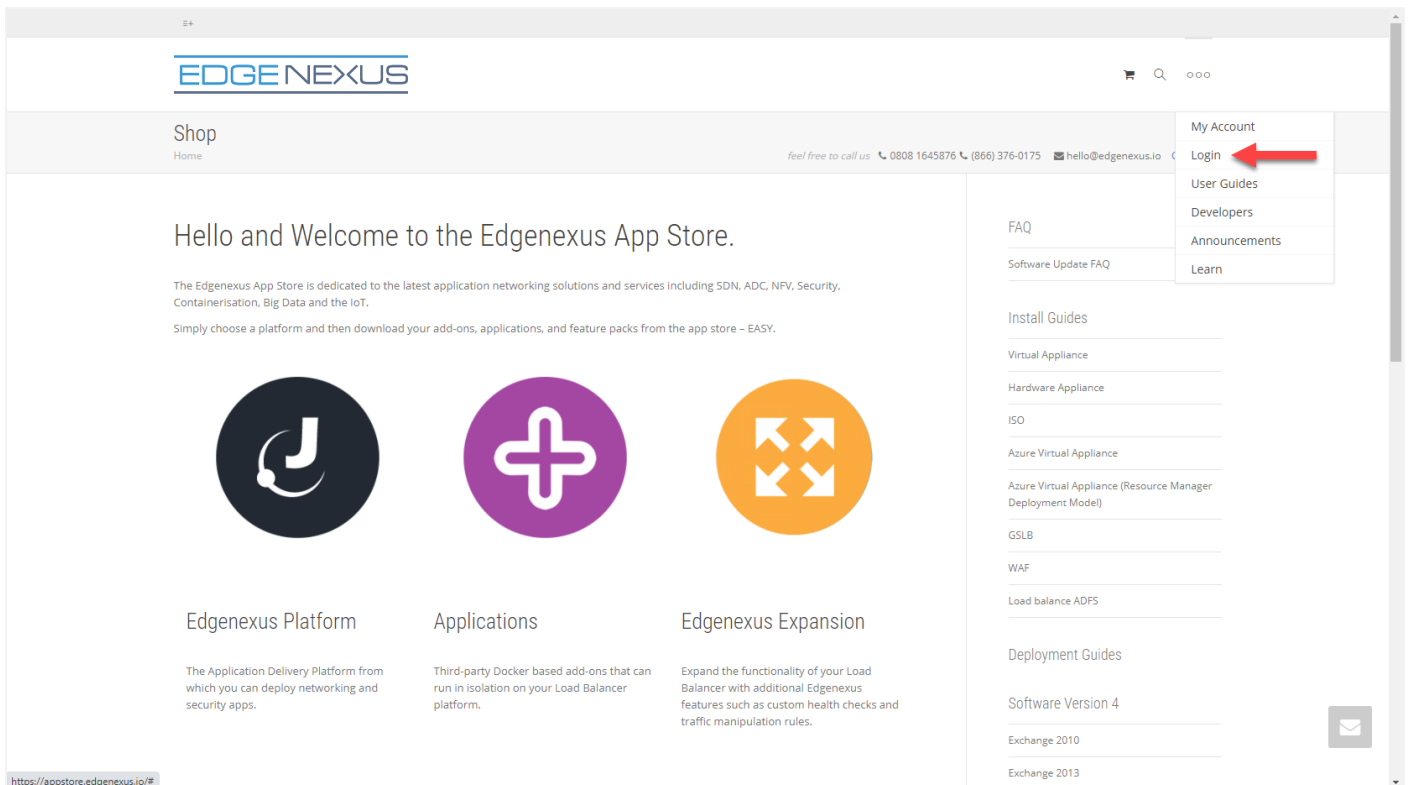
Installing the EdgeGSLB App

Getting the EdgeGSLB from the App Store

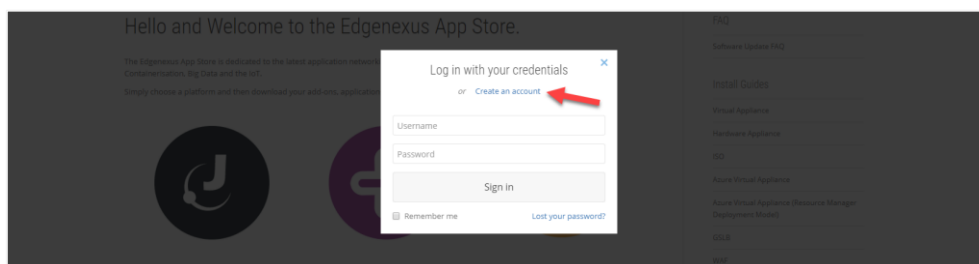
Obtaining the EdgeGSLB is very easy.

As with every Edgenexus App, the EdgeGSLB App is available through the App Store and is free of cost.

- The first thing to do is to register for access to the Edgenexus App Store. This process is done by using a browser and navigating to <https://appstore.edgenexus.io>.



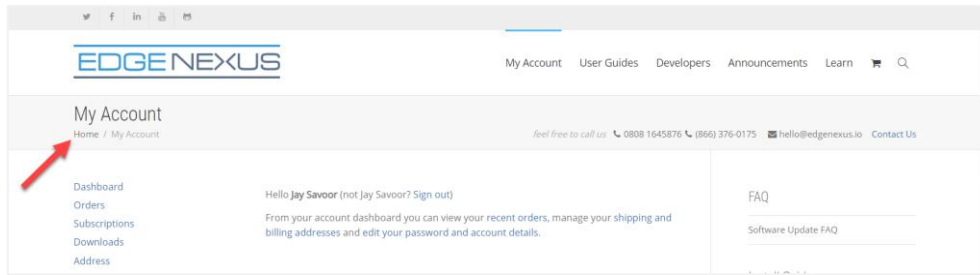
- Click on the login link in the hamburger icon at the top right.
- Click on the Create an Account, or log in using your account credentials.



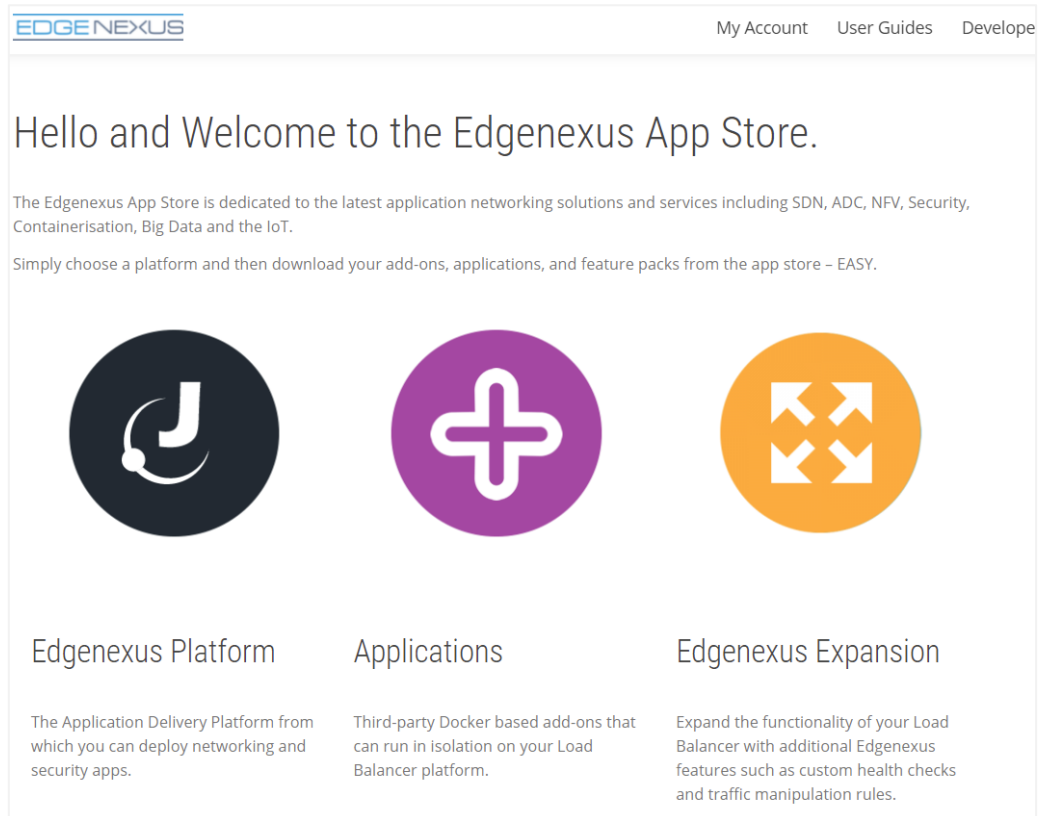
- Once you have logged in, please click on the Home link under the logo.

EdgeGSLB

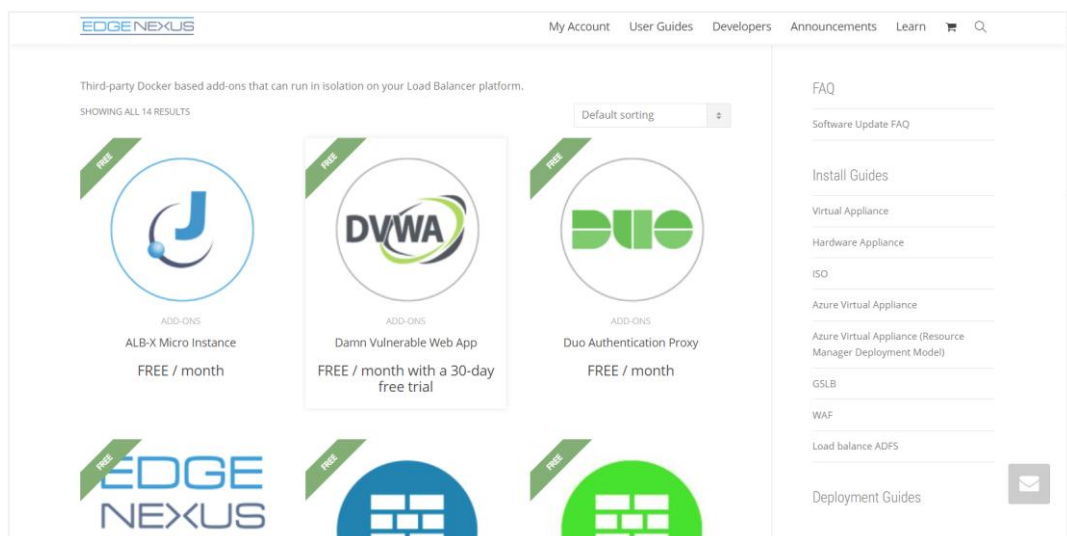
Administrator User Guide



- Next, click on Applications.



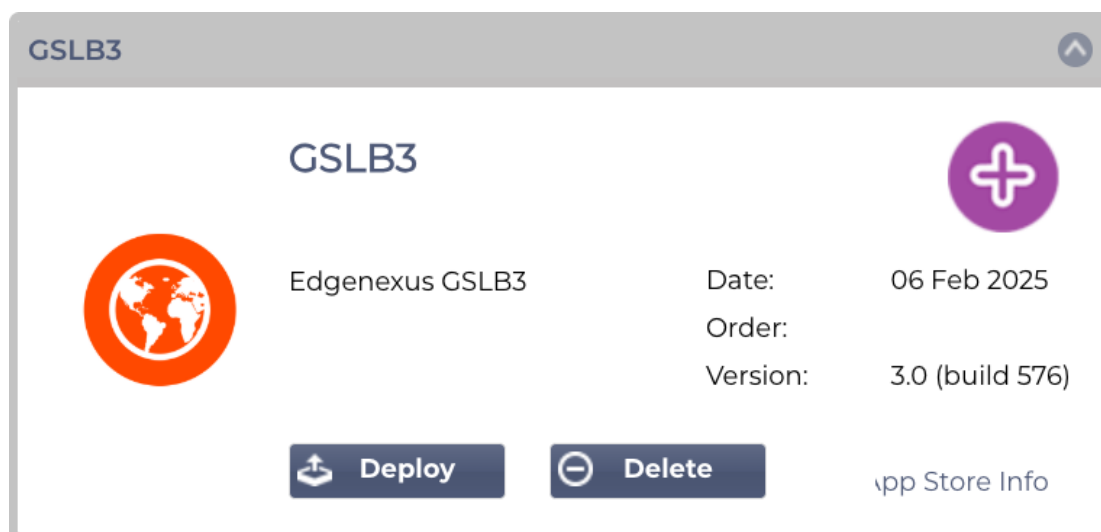
- This action will take you to the Applications page, where you can download the EdgeGSLB.



- Within the applications page, you can browse for and order the App.
- The EdgeGSLB is free to try, but you purchase it for full use.
- At this point, you have two options: Using the App Store from within the EdgeADC or directly downloading the App from the App Store and then uploading it to the EdgeADC.

Downloading and importing the App using the EdgeADC

- The first option is to log in using your App Store credentials inside the EdgeADC. The integrated App Store interface is available using Services > App Store.
- This method will allow you to make the purchase, and then find it available within the Purchased Apps section in Library > Apps.
- EdgeGSLB App looks something like the one shown below.



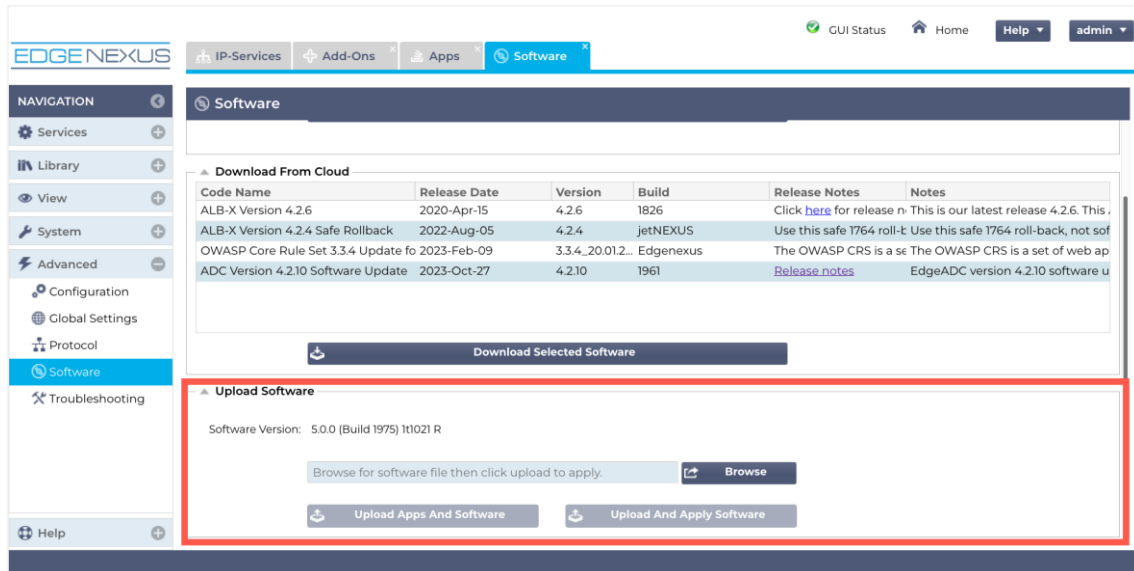
- You can then choose to download the App, and it will appear in the Downloaded Apps section.
- From the Library > Apps > Downloaded Apps section, locate the EdgeGSLB App and then deploy it to the EdgeADC containers by clicking the Deploy button.
- Once deployed, it will be available in the Library > Add-Ons tab

Download and import the App using direct download

- The secondary method uses your App Store login and directly downloads it to your desktop using a browser.
- Once downloaded, please make sure you save it without altering the filename.
- Please also ensure that there is no (1) or something similar in the filename, possibly indicating a second download, etc.
- With the file downloaded, navigate to Advanced > Software of the EdgeADC GUI using your browser.

EdgeGSLB

Administrator User Guide

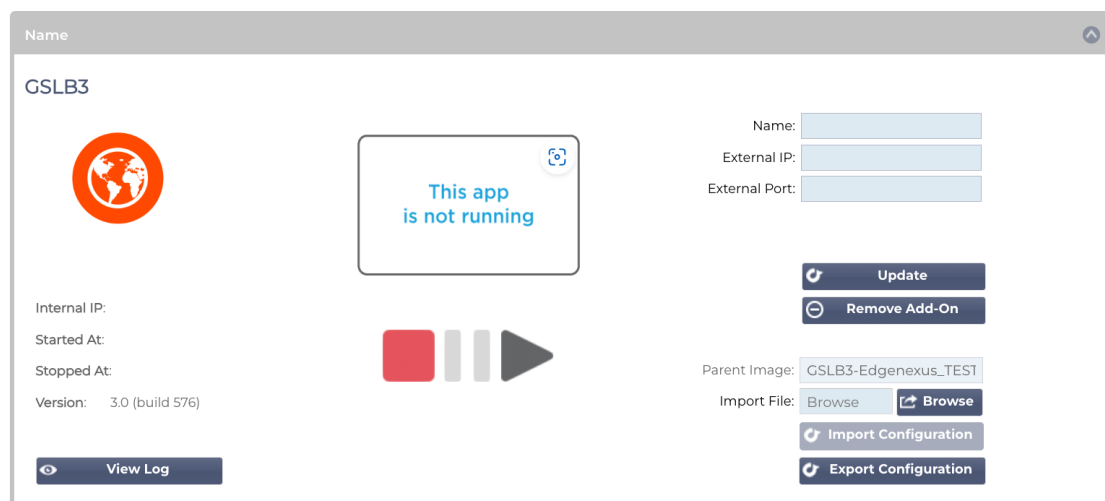


- There are several sections within the Software page, but the one we need is Upload Software.
- First, click the Browse button and find the EdgeGSLB App you downloaded.
- Next, click the Upload and Apply Software.
- The App will be shown in the Downloaded Apps section of Library > Add-Ons.
- From the Library > Apps > Downloaded Apps section, locate the EdgeGSLB App and then deploy it to the EdgeADC containers by clicking the Deploy button.
- Once deployed, it will be available in the Library > Add-Ons tab

Making the EdgeGSB App operational

When an App is downloaded and deployed, it is yet to be operational. It has to be given an IP address in the same subnet as the EdgeADC and ports through which it needs to be accessible.

- Navigate to Library > Add-Ons and locate the EdgeGSLB App.
- It should look something like the image below.



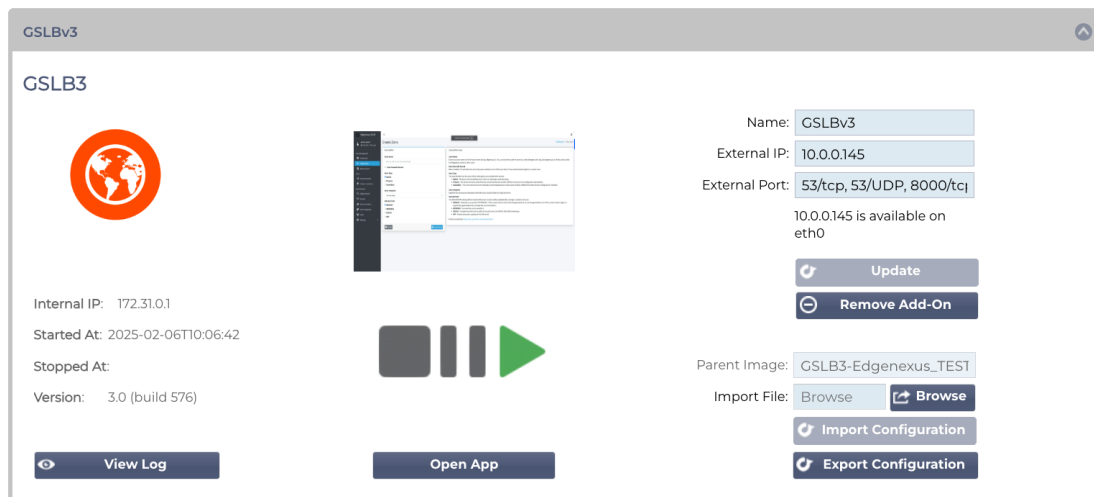
- As shown in the Container Name and External IP field, no name or IP address is allocated.
- Add an appropriate static IP address.
- Next, give the App a name – the EdgeADC's internal DNS system uses this to refer to the App when needed.

EdgeGSLB

Administrator User Guide

Note: The provision of a name is mandatory and essential for internal ADC <> GSLB communications.

- You will need to add the relevant ports for DNS. These are 53/tcp, 53/udp and 8000/tcp.
- Once you have done this, click the Update button to initialize the App.
- It should look something like the one below.



- Click the PLAY icon to activate the App into an operational state.

Note the Open App button to launch the App GUI and the Pause App and Stop App buttons.

- You can launch the App GUI using View App or the listing in the IP Services section.

The EdgeGSLB App runs within the ADC's docker container technology, ensuring its safety and integrity. The App uses a separate docker0 network to communicate with the EdgeADC load balancer. When the App is started, it is allocated an IP address from the docker0 pool. This IP address is automatically resolved by the EdgeADC using the docker name you provided in the Container Name field. You can see the internal IP address on the right side of the App.

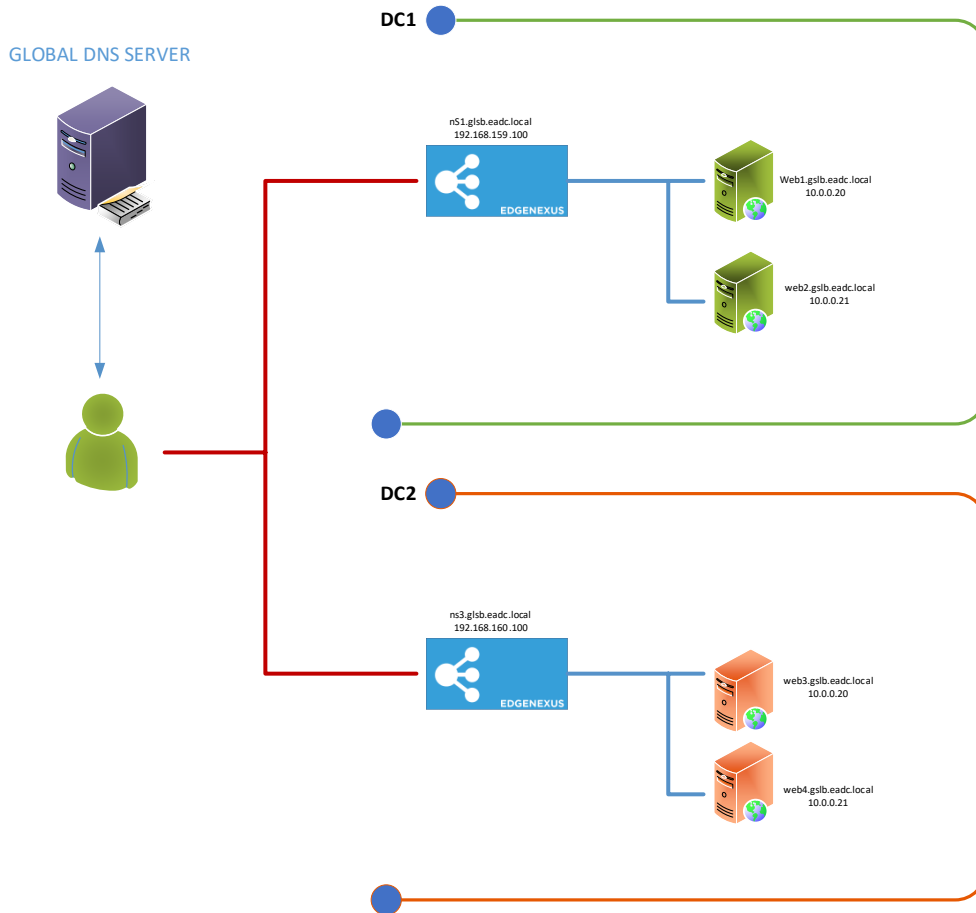
You will also need to ensure that the EdgeADC can resolve DNS names using the GSLB's PowerDNS module. The External IP address of our EdgeGSLB App, 192.168.159.124 in our example shown above, needs to be added as the Primary DNS in the System > Networking section. See the example below.



Configuring the EdgeGSLB

Example network

In this example, we are using a single ADC-based GSLB topology. We will deal with clustered Adc topologies later in this guide. See the network example below.



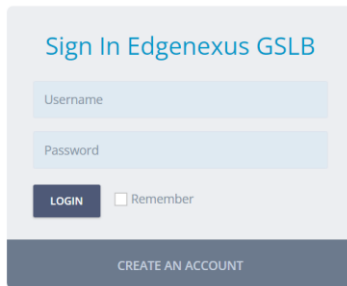
Configuring your EdgeGSLB

You will need to use your browser to access the EdgeGSLB App for the configuration needed.

To access the App, use the Add-on GUI button. You can also access this using the browser and the following URL, **https://{EXTERNAL_IP_ADDRESS}:8000**.

This action will open a browser window or tab and display the page below.

EDGE NEXUS



Sign In Edgenexus GSLB

Username

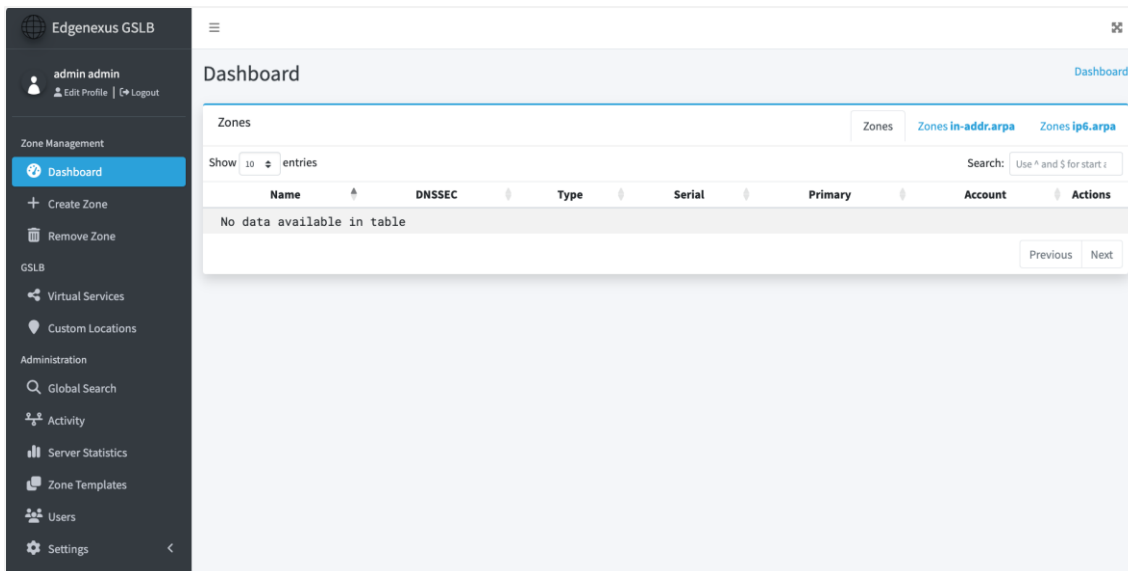
Password

☐ Remember

Edgenexus Global Server Load Balancer

The default username and password are *admin* and *jetnexus*, the same as the EdgeADC. You can change this once you have logged in.

Once logged in, you will be presented with a page similar to the one shown below.



The screenshot shows the Edgenexus GSLB Dashboard. On the left is a dark sidebar with navigation links: Zone Management (Dashboard, Create Zone, Remove Zone), GSLB (Virtual Services, Custom Locations), Administration (Global Search, Activity, Server Statistics, Zone Templates, Users, Settings). The main content area is titled 'Dashboard' and features a 'Zones' section. It includes a search bar, a table with columns: Name, DNSSEC, Type, Serial, Primary, Account, and Actions. The table currently shows 'No data available in table'. There are 'Previous' and 'Next' buttons at the bottom of the table.

As you can see, a dummy domain name has been preconfigured as an illustration.

Note: It is impossible to edit a domain entry once it has been created. You can only delete the domain entry.

This guide will show you how to configure the GSLB using the dummy configuration and will allow you to get a good idea of how to use your domain and VIP entries when configuring it for POC or production.

Adding a new zone (aka domain)

The domain (in our example, eadc.local) is entered in this stage will be the one that the GSLB uses for resolving. You may opt to use the prefix 'gslb' in front of your domain name as a subdomain, as we have in this example, and it will then be 'gslb.eadc.local'.

- Click the Create Zone button located in the left panel.
- You will see the form on the right where you can configure the zone.
- Enter your full domain name in the field shown in the example.

EdgeGSLB

Administrator User Guide

Zone Editor

Zone Name
gslb.eadc.local

☐ Zone Override Record

Zone Type
☒ Native
☐ Primary
☐ Secondary

Zone Template
No template

SOA-EDIT-API
☒ DEFAULT
☐ INCREASE
☐ EPOCH
☐ OFF

Zone Editor Help

Zone Name
Enter your zone name in the format of name.tld (eg. edgenexus.io). You can also enter sublevel zones to create delegate zones (eg. sub.edgenexus.io) which can be useful for delegating control to other users.

Zone Override Record
When enabled, this will allow the user to by-pass validation errors if the user doesn't have administration rights to a parent zone.

Zone Type
The type decides how the zone will be replicated across multiple DNS servers.

- Native** - The server will not perform any Primary or Secondary zone functions.
- Primary** - The server will serve as the Primary and will send zone transfers (AXFRs) to other servers configured as secondaries.
- Secondary** - The server will serve as the Secondary and will request and receive zone transfers (AXFRs) from other servers configured as Primaries.

Zone Template
Specifies the existing zone template which this zone should initially be replicated from.

SOA-EDIT-API
The SOA-EDIT-API setting defines how the SOA serial number will be updated after a change is made to the zone.

- DEFAULT** - Generate a soa serial of YYYYMMDD01. If the current serial is lower than the generated serial, use the generated serial. If the current serial is higher or equal to the generated serial, increase the current serial by 1.
- INCREASE** - Increase the current serial by 1.
- EPOCH** - Change the serial to the number of seconds since the EPOCH, AKA UNIX timestamps
- OFF** - Disable automatic updates of the SOA serial.

- Leave the TYPE settings in the form as they are if this is a single ADC GSLB. However, if you are using clustered scenarios or wish to a GSLB in a separate data center residing in the same network, you will need to look at the section, Primary-Secondary DNS Replication.
- Click the Create Zone button.

You should now see the following in the Dashboard.

Dashboard

Zones

Show 10 entries

Name	DNSSEC	Type	Serial	Primary	Account	Actions
gslb.eadc.local	N/A	Native	2025021001	N/A	None	

Previous 1 Next

- Click on the newly created gslb.eadc.local entry.

You will see that you have a preconfigured SOA record and the ability to enter A records required for proper operation.

You will need to enter A records for the Real Servers used for the Virtual Services and the IP addresses for the NS records, which will correspond to the VIPs that point to the GSLB.

In our example, we have the records as per the image below.

EdgeGSLB

Administrator User Guide

The screenshot shows the 'Zone Editor' for 'gslb.eadc.local'. It features a table of DNS records with columns: Name, Type, Status, TTL, Data, Comment, and Actions. The records include an SOA record for '@' and four A records for 'ns1', 'ns2', 'web1', and 'web2'. The SOA record's Data field is 'ns1.gslb.eadc.local. hostmaster.gslb.eadc.local. 20 25021002 10800 3600 604800 3600'. The A records show IP addresses for ns1 (192.168.159.100), ns2 (192.168.160.100), web1 (10.0.0.20), and web2 (10.0.0.21). The interface also includes buttons for 'Zone Settings', 'Changelog', 'Add Record', and 'Save Changes'.

Name	Type	Status	TTL	Data	Comment	Actions
@	SOA	Active	3600	ns1.gslb.eadc.local. hostmaster.gslb.eadc.local. 20 25021002 10800 3600 604800 3600		[Edit] [Delete]
ns1	A	Active	60	192.168.159.100		[Edit] [Delete] [Refresh]
ns2	A	Active	60	192.168.160.100		[Edit] [Delete] [Refresh]
web1	A	Active	60	10.0.0.20		[Edit] [Delete] [Refresh]
web2	A	Active	60	10.0.0.21		[Edit] [Delete] [Refresh]

In our example, please observe the following:

- The SOA record has been changed to assign ns1.gslb.eadc.local as the primary name server. Note the period at the end of the ns1 entry.
- We have added the IP addresses for ns1 and ns2, where ns1 is in datacenter 1, and ns2 is in datacenter 2.
- We also the A records for the real servers – we will have similar records on the second load balancer in datacenter 2.

Configuring the Associated Virtual Services

We will now switch back to the IP Services tab of the ADC, where some VIP/VS entries need to be made.

We will make three entries that correspond to the required Virtual services.

1. **GSLB DNS VIP** – This VIP is used to access the DNS server integrated into the GSLB App. The VIP needs to access DNS using port 53 TCP/UDP.

The screenshot shows the 'Virtual Services' configuration page. It includes a table with columns: Mode, VIP, VS, Ena..., IP Address, SubNet Mask / Prefix, Port, Service Name, and Service Type. Three entries are listed: 'Active' for 'GSLB DNS VS' (port 53, Layer4 TCP/UDP), 'Active' for 'gslb.eadc.local' (port 80, HTTP(S)), and 'Active' for 'GSLB UI VS' (port 8000, HTTP(S)). Below the table, there is a 'Real Servers' section with tabs for 'Server', 'Basic', 'Advanced', and 'flightPATH'. The 'Server' tab is selected, showing a table with columns: Status, Activity, Address, Port, Weight, Cal. Weight, Monitor End Point, Notes, and ID. One entry is shown: 'Online' for 'GSLBv3' (port 53, weight 100, monitor 'Self').

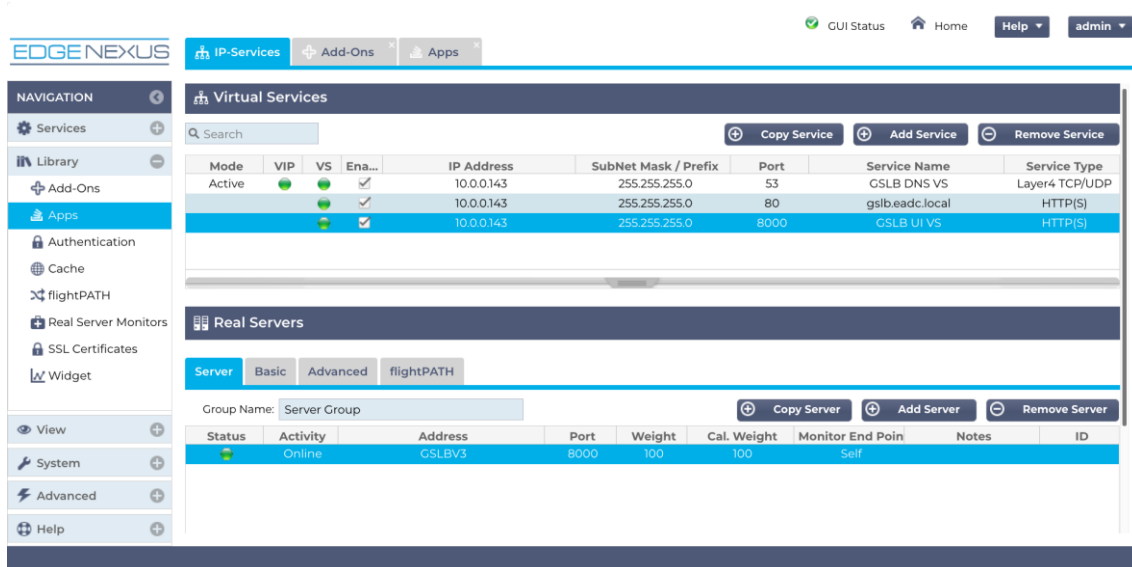
Mode	VIP	VS	Ena...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			<input checked="" type="checkbox"/>	10.0.0.143	255.255.255.0	53	GSLB DNS VS	Layer4 TCP/UDP
			<input checked="" type="checkbox"/>	10.0.0.143	255.255.255.0	80	gslb.eadc.local	HTTP(S)
			<input checked="" type="checkbox"/>	10.0.0.143	255.255.255.0	8000	GSLB UI VS	HTTP(S)

Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID
Online		GSLBv3	53	100	100	Self		

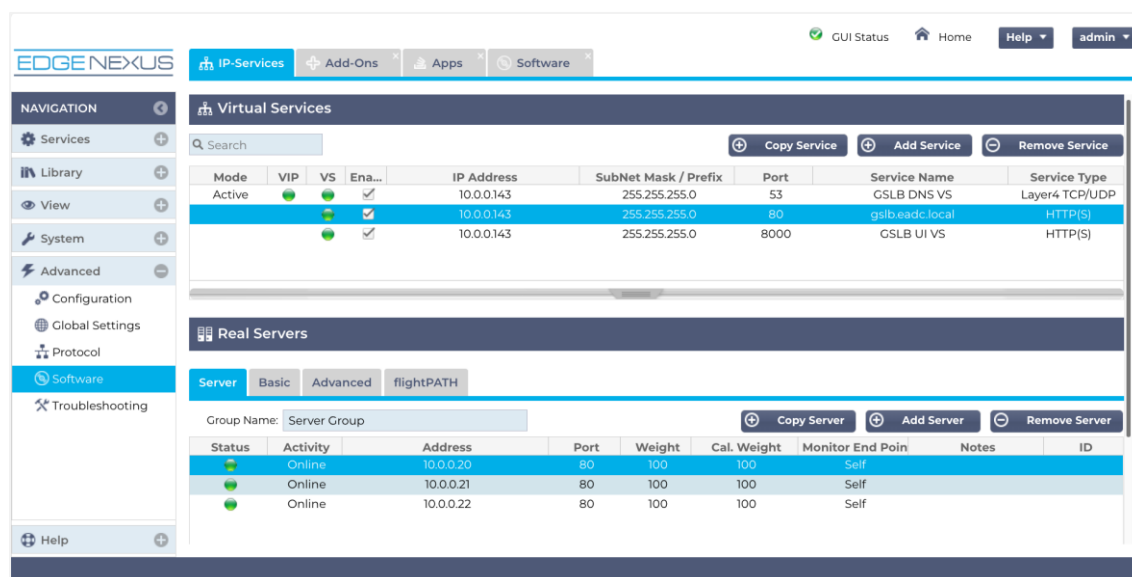
2. **GSLB UI VIP** – This VIP uses port 8000 and HTTPS services to access the admin user interface of the GSLB App. You may wish to make this VIP accessible from specific source IP ranges using flightPATH traffic rules for security measures.

EdgeGSLB

Administrator User Guide



3. **GSLB Services Health VS** – This Virtual service is critical to the operation of the GSLB as it uses health checks that you specify to determine the health of the real servers. The GSLB module uses FQDNs to access the real servers, as seen in our example.



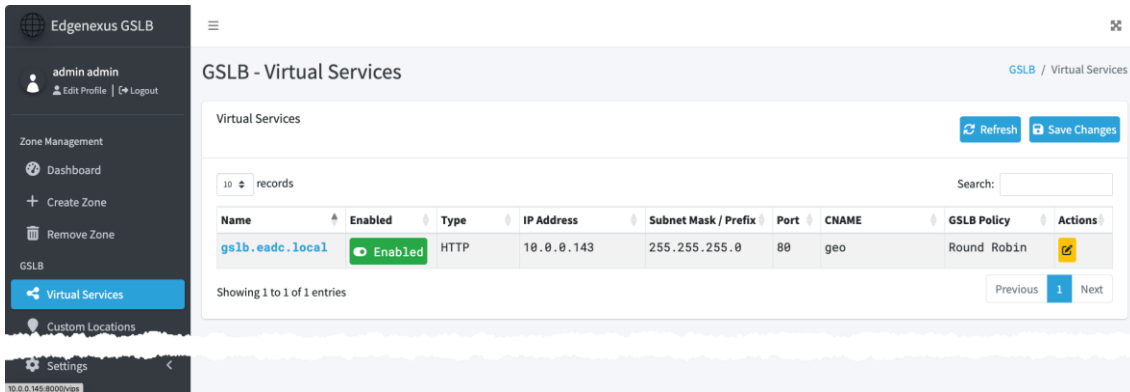
There are some important points to note when configuring the GSLB Services Health VS.

1. **Service Name** – This represents what the CNAME entry in the upstream DNS server will be pointing to resolve the IP address for the service the client is trying to access. So in our example, this will be *gslb.eadc.local*. This will be automatically read by the GSLB and displayed in the Virtual Services section.
2. **Address entries in the Real Server section** are required as the EdgeADC looks up the IP addresses relating to the hostnames configured. It does this by referring to the GSLB configured as the ADC's primary DNS server. The ADC will perform the health check configured in the Real Servers Basic tab to confirm the reachability of the returned server IP and port.

The information you enter here will be scraped by the GSLB using the EdgeADC REST API and entered in the GSLB Virtual Services section. The image below shows the Virtual Services section of the GSLB once the data has been transferred.

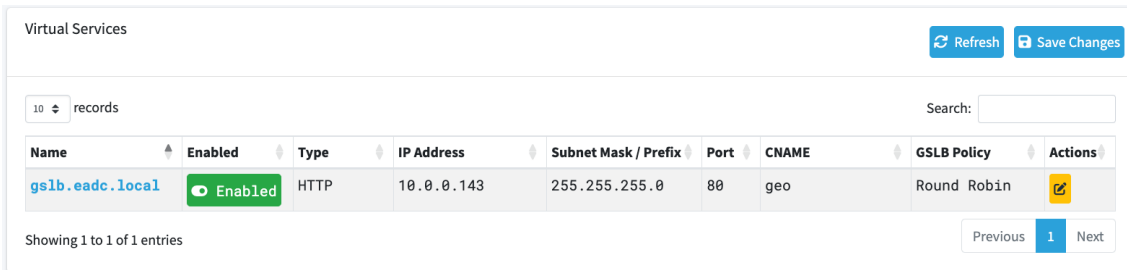
EdgeGSLB

Administrator User Guide



GSLB Virtual Services

In this section, we will describe the Virtual Services section within GSLB.



Field	Description
Name	This is the value obtained from the GSLB Services Health VS
Enabled/Disabled	This will enable or disable this Virtual Service record within GSLB. Disabling will mean that any service failure will not be detected by GSLB.
Type	This displays the service type for the VS. In this case it is HTTP, but if it were a Layer 4 VS that was defined in the GSLB it would display it as such here. The value is picked from the Services Type value defined in the Virtual Service
IP Address	This is the IP address of the VS.
Subnet Mask/Prefix	The subnet mask of the VS.
Port	The port that has been defined in the VS.
CNAME	This is generated CNAME value and can be edited to your choice by using the Actions button.
GSLB Policy	This is the policy used by the GSLB. Values available are: <div><div>Fixed Weight</div><div>Geolocation - City Match</div><div>Geolocation - Continent Match</div><div>Geolocation - Country Match</div><div>Geolocation - Proximity</div><div>✓ Round Robin</div></div>

GSLB Policies

The default GSLB policy created for the Virtual Service is Round Robin, as this is the defacto one used by DNS. As the name suggests, any queries made to the domain name will be cycled through the available hosts/IP addresses.

Clicking on the entry will display a dropdown menu, as shown below. The options available are different GSLB policies that the GSLB App supports.

Fixed Weight

Geolocation - City Match

Geolocation - Continent Match

Geolocation - Country Match

Geolocation - Proximity

✓ Round Robin

As the name suggests, these policies are all related to the client's geographical location. Depending on the source IP location, the GSLB and the EdgeADC will decide to which data centre the client requests will be sent.

Fixed Weight

The Fixed Weight policy in EdgeGSLB assigns a predefined weight to each backend server, distributing traffic proportionally based on these weights. Higher-weighted servers receive more requests, ensuring load distribution according to the specified values.

Geolocation – City Match

The Geolocation - City Match policy in EdgeGSLB is used to direct DNS queries to specific servers based on the city of the requesting client. This is part of EdgeGSLB's geolocation capabilities, which leverage MaxMind GeoIP databases or similar sources to determine the client's geographic location.

When this policy is applied, the EdgeGSLB attempts to match the client's IP address to a known city and then routes their request to the most appropriate DNS response based on predefined rules. This is particularly useful for content delivery networks (CDNs), load balancing, and improving latency by serving users from the nearest available server.

Geolocation – Continent Match

The Geolocation - Continent Match policy in EdgeGSLB ensures that DNS queries are answered with endpoints located on the same continent as the requester. If no matching endpoint is available, the policy falls back to the next best option based on configured rules. This improves latency and regional traffic distribution.

Geolocation – Proximity

The Geolocation - Proximity policy in EdgeGSLB directs users to the nearest available server based on their geographic location. It determines proximity by evaluating the network latency or geographic distance between the user and available endpoints, ensuring optimal performance and low-latency responses.

Round Robin

The Round Robin policy in EdgeGSLB distributes DNS responses in a cyclic manner among multiple configured endpoints. Each query is answered with the next available record in sequence, ensuring an even distribution of traffic across all endpoints. This method does not consider endpoint health or load.

Custom Locations

The Custom Locations feature in EdgeGSLB allows administrators to define specific geographic or network-based locations for incoming DNS queries. This feature enhances geo-aware traffic management by enabling the mapping of client IP addresses to predefined locations instead of relying solely on standard geolocation databases.

Key Aspects:

- **Manual Location Definitions** – Administrators can define custom locations using IP address ranges, ASN numbers, or other network identifiers.
- **Overrides Standard GeoIP Data** – This feature is useful when default geolocation data is incorrect or needs refinement.
- **Integration with Load Balancing Policies** – Custom locations can be used with traffic steering policies, such as Geolocation-Based Load Balancing, to ensure that queries are resolved to the closest or most appropriate endpoints.
- **Flexible Configuration** – The mappings can be configured through APIs or configuration files, depending on the deployment model.

This feature is particularly useful in scenarios where ISPs have incorrect geolocation data, where there is a need to enforce specific routing rules, or for private network environments where public GeoIP data is not applicable.

Please see the Wikipedia page explaining private addressing https://en.wikipedia.org/wiki/Private_network

How the Custom Locations feature works

Typically the idea behind using our GSLB for internal networks is that users from certain addresses will receive a different answer for a service depending on which network they are located in, so if we consider two datacentres, one called “North” and the other called “South”, providing a service called north.gslb.eadc.local and south.gslb.eadc.local respectively. When a user from the Northern data centre queries the GSLB, we want the GSLB to respond with the IP address associated with north.gslb.eadc.local, provided the service is working correctly. Alternatively, if a user from the Southern data centre queries the GSLB, we want the GSLB to respond with the IP address associated with south.gslb.eadc.local again, providing the service is working properly.

So what do we need to do to make the above scenario work?

1. We need to have at least two Custom Locations, one for each data centre
2. Assign the various private networks to these locations
3. Assign each service to the respective location

How do we configure this scenario on the GSLB?

1. Add a location for the Northern Data Center
 - Click on Custom Locations on the left-hand side
 - Click Add Location
 - Name = North
 - Add a private IP address and subnet mask for your Northern network. For this exercise, we will assume that the service and the client IP addresses are in the same private network, 10.1.1.0/24
 - Continent Code = Europe
 - Country Code = UK
 - City = Enfield
 - Latitude (obtained from Google) = 51.6523
 - Longitude (obtained from Google) = 0.0807





Note: Please use the correct code, which can be obtained [here](#)

Add a location for the Southern Data Center

- Click on Custom Locations on the left-hand side
- Click Add Location
- Name = South
- Add a private IP address and subnet mask for your Southern network. For this exercise, we will assume that the service and the client IP addresses are in the same private network. 192.168.1.0/24
- Continent Code = Europe
- Country Code = UK
- City = Croydon
- Latitude (obtained from Google) = 51.3762
- Longitude (obtained from Google) = 0.0982

Note: Please use the correct code, which can be obtained [here](#)

The result should appear something like the image below.

Name	IP Address	Subnet Mask / Prefix	Continent	Country	City	Latitude	Longitude	Actions
North	10.1.1.0	24	Europe	GB	Enfield	51.6523	0.0007	 
South	192.168.1.0	24	Europe	GB	Croydon	51.3762	0.0982	 

Adding A Records for the custom locations

Add an A record for north.gslb.eadc.local

- Click on the domain gslb.eadc.local
- Click Add Record
- Name = North
- Type = A
- Status = Active
- TTL = 1 Minute
- IP Address = 10.1.1.254
(Note this is in the same network as the location Enfield)





















Add an A record for south.gslb.eadc.local

- Click on the domain gslb.eadc.local
- Click Add Record
- Name = South
- Type = A
- Status = Active
- TTL = 1 Minute
- IP Address = 192.168.1.254
(Note this is in the same network as the location Croydon)

The final table should look like the image below.

EdgeGSLB

Administrator User Guide

Zone Editor							
				Zone Settings	Changelog	+ Add Record	Save Changes
10 records	Search: <input type="text"/>						
Name	Type	Status	TTL	Data	Comment	Actions	
@	SOA	Active	3600	ns1.gslb.eadc.local. hostmaster.gslb.eadc.local. 2025021101 10800 3600 604800 3600		 	
north	A	Active	60	10.1.1.254		  	
ns1	A	Active	60	192.168.159.100		  	
ns2	A	Active	60	192.168.160.100		  	
south	A	Active	60	192.168.1.254		  	
web1	A	Active	60	10.0.0.20		  	
web2	A	Active	60	10.0.0.21		  	
Showing 1 to 7 of 7 entries						Previous	Next

Traffic Flow

Example 1 – Client in Northern Data-Center

1. Client IP 10.1.1.23 queries GSLB for gslb.eadc.local
2. GSLB looks up the IP address 10.1.1.23 and matches it with Custom Location Enfield 10.1.1.0/24
3. GSLB looks at its A records for the gslb.eadc.local and matches north.gslb.eadc.local as it is also in the network 10.1.1.0/24
4. GSLB responds to 10.1.1.23 with the IP address 10.1.1.254 for gslb.eadc.local

Example 2 – Client in Southern Data-Center

1. Client IP 192.168.1.23 queries GSLB for gslb.eadc.local
2. GSLB looks up the IP address 192.168.1.23 and matches it with Custom Location Croydon 192.168.1.0/24
3. GSLB looks at its A records for the gslb.eadc.local and matches south.gslb.eadc.local as it is also in the network 192.168.1.0/24
4. GSLB responds to 192.168.1.23 with the IP address 192.168.1.254 for gslb.eadc.local

Primary-Secondary DNS Replication

The Primary-Secondary GSLB record replication using AXFR feature in EdgeGSLB enables the transfer of DNS zone data from a primary GSLB instance to one or more secondary GSLB instances using the AXFR (Authoritative Zone Transfer) protocol. This ensures synchronization of global server load balancing (GSLB) records across multiple locations for redundancy and consistency.

How It Works

Primary GSLB Configuration

The primary GSLB instance holds the authoritative zone data.

It allows AXFR requests from designated secondary GSLB instances.

Zone updates (e.g., new records, changes in load balancing policies) are maintained on the primary.

Secondary GSLB Configuration

The secondary GSLB instances are configured to request and receive full zone transfers from the primary using AXFR.

These instances act as read-only replicas, ensuring that DNS queries served from different locations remain consistent.

AXFR Transfer Process

When a secondary GSLB instance starts or detects a zone update, it sends an AXFR request to the primary.

The primary responds with the entire zone file, ensuring all records are copied accurately.

If IXFR (Incremental Zone Transfer) is supported and configured, only changes are transferred instead of the entire zone.

Failover & Load Distribution

In case the primary becomes unreachable, secondary instances continue serving the last synchronized records.

Load balancing decisions remain consistent across multiple geographically distributed GSLB nodes.

Key Benefits

- Ensures high availability by replicating GSLB data across multiple locations.
- Reduces manual configuration efforts by automating synchronization.
- Supports disaster recovery by allowing secondary GSLB instances to serve queries if the primary fails.
- Optimizes performance by distributing query loads across multiple servers.

This AXFR-based replication mechanism is essential for maintaining a resilient, synchronized, and geographically distributed GSLB architecture in EdgeGSLB.

Setting up the Primary and Secondary(s)

To set up Primary-Secondary replication, you must first specify the Primary GSLB followed by any Secondary GSLB module(s).

To do this, ensure you click the Primary radio button when creating the domain. This will ensure that this GSLB becomes the Primary. This setting cannot be changed once the domain is created.

Create Zone

Zone Editor

Zone Name
Enter a valid zone name (required)

☐ Zone Override Record

Zone Type
☐ Native
☒ Primary
☐ Secondary

Zone Template
No template

SOA-EDIT-API
☒ DEFAULT
☐ INCREASE
☐ EPOCH
☐ OFF

Cancel Create Zone

Zone Editor Help

Zone Name
Enter your zone name in the format of name.tld (eg. edgenexus.io). You can also enter sublevel zones to create delegate zones (eg. sub.edgenexus.io) which can be useful for delegating control to other users.

Zone Override Record
When enabled, this will allow the user to by-pass validation errors if the user doesn't have administration rights to a parent zone.

Zone Type
The type decides how the zone will be replicated across multiple DNS servers.

- Native** - The server will not perform any Primary or Secondary zone functions.
- Primary** - The server will serve as the Primary and will send zone transfers (AXFRs) to other servers configured as secondaries.
- Secondary** - The server will serve as the Secondary and will request and receive zone transfers (AXFRs) from other servers configured as Primaries.

Zone Template
Specifies the existing zone template which this zone should initially be replicated from.

SOA-EDIT-API
The SOA-EDIT-API setting defines how the SOA serial number will be updated after a change is made to the zone.

- DEFAULT** - Generate a soa serial of YYYYMMDD01. If the current serial is lower than the generated serial, use the generated serial. If the current serial is higher or equal to the generated serial, increase the current serial by 1.
- INCREASE** - Increase the current serial by 1.
- EPOCH** - Change the serial to the number of seconds since the EPOCH, AKA UNIX timestamps
- OFF** - Disable automatic updates of the SOA serial.

Find more details at <https://doc.powerdns.com/authoritative/>

Once you have configured the Primary, the next step will be to create and configure the Secondary(s). The same step shown in the image above is used when you create the domain on the Secondary GSLB, except for selecting the Secondary radio button (see image below).

Create Zone

Zone Editor

Zone Name
Enter a valid zone name (required)

☐ Zone Override Record

Zone Type
☐ Native
☒ Primary
☐ Secondary

Zone Template
No template

SOA-EDIT-API
☒ DEFAULT
☐ INCREASE
☐ EPOCH
☐ OFF

Cancel Create Zone

Zone Editor Help

Zone Name
Enter your zone name in the format of name.tld (eg. edgenexus.io). You can also enter sublevel zones to create delegate zones (eg. sub.edgenexus.io) which can be useful for delegating control to other users.

Zone Override Record
When enabled, this will allow the user to by-pass validation errors if the user doesn't have administration rights to a parent zone.

Zone Type
The type decides how the zone will be replicated across multiple DNS servers.

- Native** - The server will not perform any Primary or Secondary zone functions.
- Primary** - The server will serve as the Primary and will send zone transfers (AXFRs) to other servers configured as secondaries.
- Secondary** - The server will serve as the Secondary and will request and receive zone transfers (AXFRs) from other servers configured as Primaries.

Zone Template
Specifies the existing zone template which this zone should initially be replicated from.

SOA-EDIT-API
The SOA-EDIT-API setting defines how the SOA serial number will be updated after a change is made to the zone.

- DEFAULT** - Generate a soa serial of YYYYMMDD01. If the current serial is lower than the generated serial, use the generated serial. If the current serial is higher or equal to the generated serial, increase the current serial by 1.
- INCREASE** - Increase the current serial by 1.
- EPOCH** - Change the serial to the number of seconds since the EPOCH, AKA UNIX timestamps
- OFF** - Disable automatic updates of the SOA serial.

Find more details at <https://doc.powerdns.com/authoritative/>

Configuring for DNS Replication

Let's assume you have created your Primary and the Secondary GSLB modules. The method below works for an HA pair and cross-data centre replication. The only proviso for multiple data centre usage is that all the GSLB modules must be able to see and talk to each other.

Log onto the Primary GSLB and proceed to Admin > Settings > AXFR, located in the side menu bar. You will see something like the example below.

EdgeGSLB

Administrator User Guide

admin admin | Edit Profile | Logout

Zone Management

- Dashboard
- Create Zone
- Remove Zone

GSLB

- Virtual Services
- Custom Locations

Administration

- Global Search
- Activity
- Server Statistics
- Zone Templates
- Users
- Settings**
- AXFR Settings
- Global Settings

AXFR Settings

Nameservers allowed to request AXFR zone transfers

#	IP address	NS	AXFR
1	10.0.0.148	10.0.0.148	<input type="checkbox"/>
2	10.0.0.149	10.0.0.149	<input type="checkbox"/>

Save Settings

AXFR Settings Help

First create domains, NS and A records in the Zone Management menu.

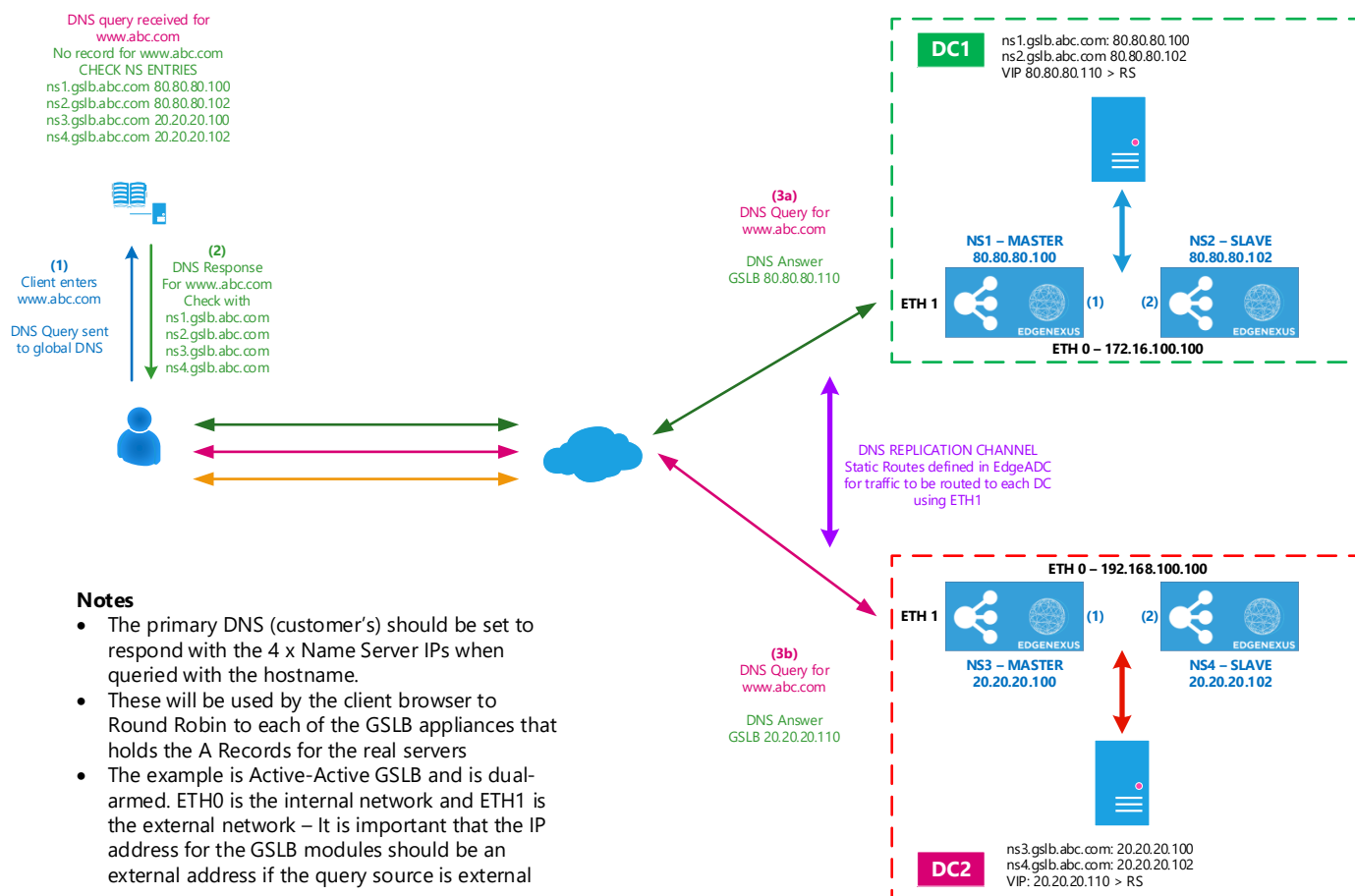
Then select addresses of the nameservers which are allowed to request DNS zone transfers (AXFR) from this Primary DNS server in order to make Primary-Secondary DNS zone replication possible.

- Tick the checkbox against the IP address of the name servers that are allowed to request AXFR zone transfers.
- Click the Save button once the entry has been completed.

This will now begin the replication process from Primary to the Secondary.

Dual Data Centre – Dual Arm Example

Sometimes, you may require an Active-Active GSLB architecture that crosses data centres. In the drawing below, we have outlined an example of two data centres with external and internal networks.



So let's see what we have in this example.

- The user in this example wishes to access a website called www.abc.com (not ABC NEWS!).
- They enter this into their browser, which queries their central DNS for the IP address.
- The central DNS responds to the user's machine that it does not have the IP address for www.abc.com, but it does have a list of Name Servers that may have the IP address for www.abc.com.
- It responds (in the example) with `ns1.gslb.abc.com`, `ns2.gslb.abc.com`, `ns3.gslb.abc.com` and `ns4.gslb.abc.com`.
- These Name Servers correspond to `gslb1` and `gslb2` in DC1 and `gslb3` and `gslb4` in DC2.
- DNS records on NS1 and NS3 Masters will be automatically replicated to NS2 and NS4, respectively.
- You could also have a single Master, say NS1 and the remaining GSLBs as Slaves. The Master will then replicate the records to the Slaves when updates are made. It is important to note that ANY changes to the records are only made on the Master. Also, it is important to understand that should the Master fail; it will need to be brought back up to make record changes.

When you wish to replicate DNS entries from the Master to Slaves that sit across data centres, you must add static routes that are fixed to use ETH1. The routes can be added in the System > Networking section.















Zone Settings

This section handles the Zone Settings that you need to use to ensure the zone is properly accessible. To access Zone Settings, click the Zone name in the Dashboard. This will display the details for the Zone.

Zone Editor

10 records

Search:

Name	Type	Status	TTL	Data	Comment	Actions
@	SOA	Active	3600	ns1.gslb.eadc.local. hostmaster.gslb.eadc.local. 2025021101 10000 3600 604800 3600		 
north	A	Active	60	10.1.1.254		 
ns1	A	Active	60	192.168.159.100		 
ns2	A	Active	60	192.168.160.100		 
south	A	Active	60	192.168.1.254		 
web1	A	Active	60	10.0.0.20		 
web2	A	Active	60	10.0.0.21		 

Showing 1 to 7 of 7 entries

Previous 1 Next

- Click the Zone Settings button indicated in the image above.

There are several sections to the Zone Settings.

Allow PTR Creation

This allows the creation of the appropriate Reverse Pointer, allowing access to the FQDN via the use of the IP address.

Auto PTR creation

☐

Allow automatic reverse pointer creation on record updates?

DynDNS 2 Settings

Allow the creation of records on-the-fly using DynDNS updates.

DynDNS 2 Settings

☐

Allow on-demand creation of records via DynDNS updates?

Zone Access Control

Configure individual zones with their own users. Zones can have multiple users so they are able to manage zones. Admin users are shown in Red and have access to all zones.

Zone Access Control

Users on the right have access to manage the records in the gslb.eadc.local zone.

Click on users to move from between columns.

Users in **red** are Administrators and already have access to **ALL** zones.

Username

↔

Username

admin

Save Changes

Change Zone Type

Using this setting, you can change the Zone type. Settings available are Native (default), Primary and Secondary.

Change Zone Type

The type decides how the zone will be replicated across multiple DNS servers.

- Native - the server will not perform any replication. Use this if you only have one server or you handle replication via your backend.
- Primary - the server will serve as the primary and will send zone transfers (AXFRs) to other servers configured as secondaries.
- Secondary - the server will serve as the secondaries and will request and receive zone transfers (AXFRs) from other servers configured as primaries.

New Zone Type Setting:

Native

Update Zone Type

A description for each option is shown in the image above.

Change SOA-EDIT-API

Change SOA-EDIT-API

The SOA-EDIT-API setting defines how the SOA serial number will be updated after a change is made to the zone.

- DEFAULT - Generate a soa serial of YYYYMMDD01. If the current serial is lower than the generated serial, use the generated serial. If the current serial is higher or equal to the generated serial, increase the current serial by 1.
- INCREASE - Increase the current serial by 1.
- EPOCH - Change the serial to the number of seconds since the EPOCH, aka unixtime.
- OFF - Disable automatic updates of the SOA serial.

New SOA-EDIT-API Setting:

DEFAULT

Update SOA-EDIT-API

A description of function and operability is shown in the image above.

Remove Zone

Remove Zone

This function is used to remove a zone from Edgenexus GSLB **AND** PowerDNS. All records and user privileges associated with this zone will also be removed. This change cannot be reverted.

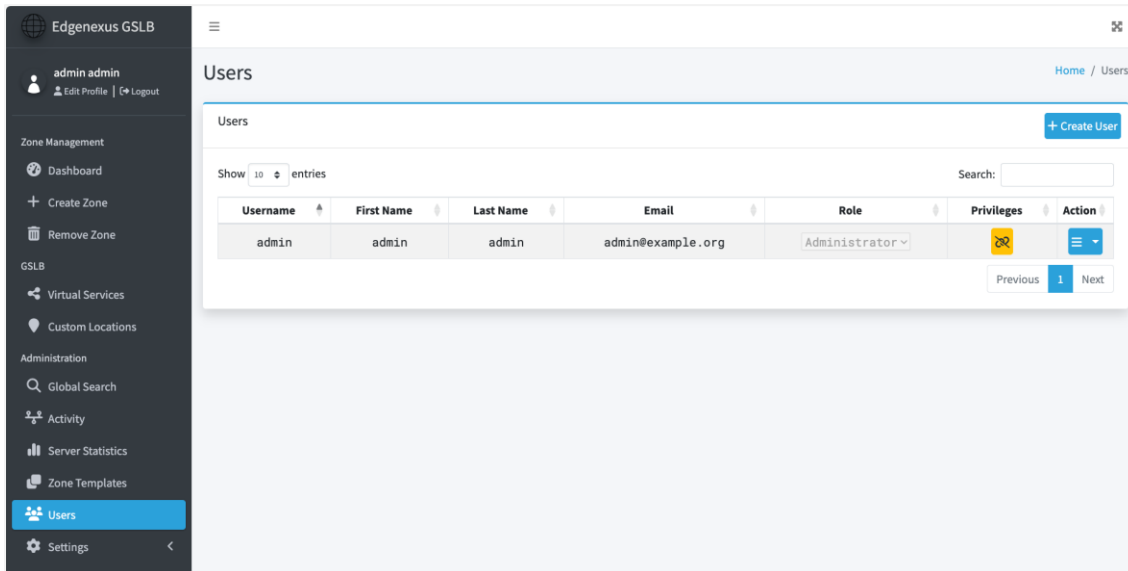
 Delete Zone

Take care with this function as it will delete the Zone and all records within. There is no reversal of this action.

Administration

Users

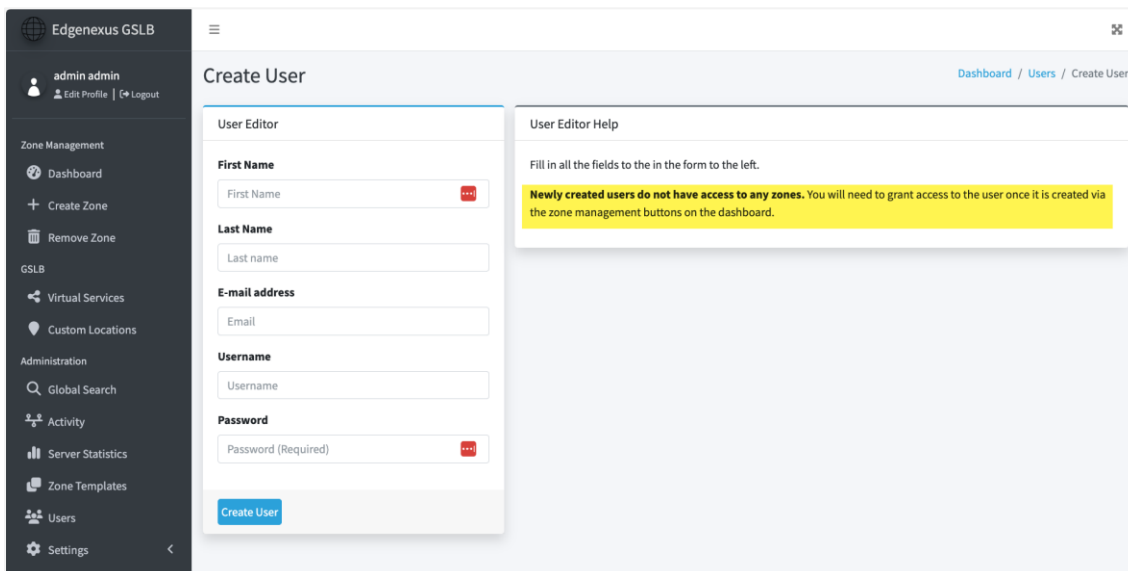
Like any application, the EdgeGSLB has the ability to add users who can access not just the entire system, but individual zones.



By default the administrator user is called admin, and the credential is jetnexus, the same as the EdgeADC's default password.

Creating a User

Click the Create User button shown above.



It is vital to take note of the section highlighted within the image in yellow. When you create a user, you need to grant access to the new user within every zone he is entitled to access.

This is done using the Zone Settings editor accessible by clicking on the zone name.

EdgeGSLB

Administrator User Guide

Zones							Zones	Zones in-addr.arpa	Zones ip6.arpa
Show 10 entries							Search: Use ^ and \$ for start & end		
Name	DNSSEC	Type	Serial	Primary	Account	Actions			
eadc1.jet.io		Primary	2025021103	N/A	None				
eadc2.jet.io		Secondary	0	10.0.0.145	None				
gslb.eadc.local		Native	2025021101	N/A	None				
							Previous	1	Next

Clicking the button displays a menu from which a number of functions can be accessed. Please check the section under Zone Management for precise instructions.

Activity

The Activity page provides an audit trail of all activities performed on the GSLB.

The screenshot shows the 'Activity' page in the EdgeGSLB Administrator. On the left is a sidebar with navigation links: Zone Management, Dashboard, Create Zone, Remove Zone, GSLB, Virtual Services, Custom Locations, Administration, Global Search, Activity (selected), Server Statistics, Zone Templates, Users, and Settings. The main content area has an 'Activity Search' section with a search bar and buttons for 'Search By Zone' and 'Search for User Authentication'. Below this are filter fields for 'Changed by:', 'Minimum date:', and 'Maximum date:', along with 'Search' and 'Clear Filters' buttons. A 'Clear Activity' button is in the top right. The activity list shows three entries:

Time	Content	Changed by	Detail
2025-02-11 12:02:22	User admin authentication succeeded	System	Info
2025-02-11 11:24:35	Apply record changes to zone eadc1.jet.io	admin	Info
2025-02-11 11:24:03	Apply record changes to zone eadc1.jet.io	admin	Info

Clicking on the Info icon shows a detailed view of the audit item.

The screenshot shows the 'Activity' page with a 'History Details' modal open. The modal displays the following information:

Name	Type	TTL	Data	Status	Comment
+ns2.eadc1.jet.io.	+NS	+60	+10.0.0.149.	+Activated	

The background activity list is dimmed, showing the same three entries as the first screenshot.

You can also search by Zone and by User Authentication.

Server Statistics

As its name suggests, this page delivers information about the GSLB server.



Statistic	Value
backend-latency	1
backend-queries	90
cache-latency	0
corrupt-packets	0
cpu-iowait	75858
cpu-steal	0
deferred-cache-inserts	0
deferred-cache-lookup	0
deferred-packetcache-inserts	0
deferred-packetcache-lookup	0

Each of the parameters is a hyperlink that will open the document search page in PowerDNS, the authoritative DNS used in the EdgeGSLB.

Description in brief

General Metrics

- latency (average query latency in microseconds) – The average response time for DNS queries, measured in microseconds. This indicates how quickly the system processes queries.
- packetcache-hit (packet cache hit count) – Number of DNS queries that were answered directly from the packet cache, avoiding further processing.
- packetcache-miss (packet cache miss count) – Number of DNS queries that were not found in the packet cache and required additional processing.
- query-cache-hit (query cache hit count) – Number of queries answered from the query cache, which stores previous DNS lookups to speed up responses.
- query-cache-miss (query cache miss count) – Number of queries not found in the query cache, requiring a backend lookup.

Query Handling

- udp-queries (total UDP queries received) – The total number of DNS queries received over UDP, the primary transport protocol for DNS.
- tcp-queries (total TCP queries received) – The total number of DNS queries received over TCP, often used for large responses or DNSSEC.
- dnssec-queries (total DNSSEC queries received) – The number of queries requesting DNSSEC-related information, such as DS or RRSIG records.
- recursing-queries (total recursive queries handled) – The number of queries that required recursive resolution, where the system had to query other DNS servers for an answer.
- servfail-answers (total SERVFAIL responses sent) – The number of queries that resulted in a SERVFAIL response, typically due to a backend failure or configuration issue.

Response Handling

- udp-responses (total UDP responses sent) – The total number of DNS responses sent over UDP.

- tcp-responses (total TCP responses sent) – The total number of DNS responses sent over TCP.
- nx-answers (total NXDOMAIN responses sent) – The number of queries that resulted in an NXDOMAIN response, indicating the requested domain does not exist.
- nxdomain-answers (total NXDOMAIN answers sent) – Another counter tracking NXDOMAIN responses separately.
- noerror-answers (total NOERROR responses sent) – The number of queries answered successfully with a NOERROR response.
- nodatattl (TTL for records without data) – The configured time-to-live (TTL) value for responses that contain no data (e.g., NOERROR but no records).

Cache Performance

- cache-entries (current cache entry count) – The total number of records stored in the cache.
- cache-hits (total cache hits) – The number of queries answered directly from cache, improving response time.
- cache-misses (total cache misses) – The number of queries that were not found in cache and required backend resolution.

Backend & Database

- backend-queries (total backend queries sent) – The number of queries forwarded to the backend data source (e.g., a database or external resolver).
- backend-answers (total backend responses received) – The number of valid responses received from the backend after a query was forwarded.
- queries-per-second (current queries per second rate) – The number of DNS queries being processed per second in real time.
- uptime (server uptime in seconds) – The duration since the EdgeGSLB server started, measured in seconds.

Performance & Stability

- cpu-usage (current CPU usage percentage) – The percentage of CPU resources currently being used by the EdgeGSLB process.
- corrupt-packets (total corrupt packets received) – The number of malformed or invalid DNS packets received and discarded.
- udp-drops (total UDP packets dropped) – The number of UDP packets dropped due to issues like rate limiting or overload.
- tcp-drops (total TCP connections dropped) – The number of TCP connections dropped, usually due to resource constraints or client timeouts.
- overload-drops (total queries dropped due to overload) – The number of queries that were dropped due to the system being overloaded beyond its capacity.

Example Scenarios

Scenario 1: High Query Latency (Slow DNS Responses)

Relevant Metrics:

- latency (average query latency in microseconds)
- backend-queries (total backend queries sent)
- cache-misses (total cache misses)
- cpu-usage (current CPU usage percentage)

Recommendations:

- **Enable caching aggressively** – A high cache-misses rate indicates queries aren't being served from cache. Increase cache TTL and size to reduce backend lookups.
- **Optimize backend performance** – If backend-queries is high, ensure the backend (e.g., database) is optimized and responsive.

- **Monitor CPU usage** – If cpu-usage is high, consider adding more CPU resources or optimizing configurations.
- **Use packet cache** – The packet cache can serve complete responses quickly and reduce latency.

Scenario 2: High Backend Load

Relevant Metrics:

- backend-queries (total backend queries sent)
- backend-answers (total backend responses received)
- query-cache-miss (query cache miss count)

Recommendations:

- **Optimize query caching** – Reduce the frequency of backend lookups by adjusting query TTL and cache retention settings.
- **Implement rate limiting** – If excessive backend queries are caused by abuse or misconfiguration, use rate limiting policies.
- **Review zone data freshness** – Ensure the backend database or zone files are preloaded with commonly queried data.

Scenario 3: Frequent DNS Failures (SERVFAIL)

Relevant Metrics:

- servfail-answers (total SERVFAIL responses sent)
- backend-queries (total backend queries sent)
- cache-misses (total cache misses)

Recommendations:

- **Check backend availability** – Frequent servfail-answers can indicate backend failures. Verify database connectivity and health.
- **Increase cache TTL** – If backend instability is an issue, caching common queries longer can reduce downtime.
- **Validate DNSSEC settings** – If DNSSEC is enabled and servfail-answers is high, check for misconfigurations in signatures or trust chains.

Scenario 4: High NXDOMAIN Responses (Non-Existent Domains)

Relevant Metrics:

- nx-answers (total NXDOMAIN responses sent)
- nxdomain-answers (total NXDOMAIN answers sent)

Recommendations:

- **Check for misconfigured clients** – High nx-answers could indicate clients querying for incorrect domain names.
- **Consider wildcard DNS records** – If some non-existent domains should resolve, configure wildcard records in the zone.
- **Monitor for potential DDoS attacks** – A sudden increase in NXDOMAIN responses might be a sign of an attack.

Scenario 5: High Number of Dropped Queries

Relevant Metrics:

- udp-drops (total UDP packets dropped)
- tcp-drops (total TCP connections dropped)
- overload-drops (total queries dropped due to overload)
- cpu-usage (current CPU usage percentage)

Recommendations:

- **Increase server capacity** – If the system is overloaded, add more CPU, memory, or deploy additional EdgeGSLB instances.
- **Enable rate limiting** – Use rate-limiting rules to prevent abuse from excessive queries.
- **Optimize network settings** – If TCP or UDP drops are high, adjust buffer sizes and connection limits.
- **Analyze traffic patterns** – If specific clients are overloading the server, consider blocking or throttling them.

Scenario 6: Poor Cache Performance

Relevant Metrics:

- cache-entries (current cache entry count)
- cache-hits (total cache hits)
- cache-misses (total cache misses)

Recommendations:

- **Increase cache size** – A low number of cache-entries suggests the cache may be too small to be effective.
- **Extend TTL settings** – If cache-misses is high, consider increasing the TTL for commonly queried records.
- **Enable packet cache** – Packet caching can further reduce the need to reprocess queries.

Scenario 7: High Volume of Corrupt Packets

Relevant Metrics:

- corrupt-packets (total corrupt packets received)

Recommendations:

- **Check for misconfigured clients** – Some clients may be sending malformed DNS queries.
- **Analyze network traffic** – A sudden increase in corrupt packets may indicate an attack or network issue.
- **Enable logging for debugging** – Capture packet logs to identify the source of corruption.

Scenario 8: High Number of DNSSEC Queries

Relevant Metrics:

- dnssec-queries (total DNSSEC queries received)
- latency (average query latency in microseconds)

Recommendations:

- **Ensure DNSSEC is properly configured** – If queries are failing, validate DNSSEC settings and signatures.
- **Optimize cryptographic performance** – If latency increases, consider using hardware acceleration or better algorithms.

Zone Templates

The Zone Templates feature in EdgeGSLB Admin 0.4.2 allows administrators to create predefined templates for DNS zones, streamlining the process of adding new zones with consistent settings. This feature is particularly useful for organizations managing multiple zones that require a standardized set of records.

Key Features of Zone Templates

- **Predefined Records** – Each template can include a set of default DNS records, such as A, AAAA, CNAME, MX, NS, TXT, and others, ensuring new zones are preconfigured with essential records.
- **Automatic Zone Provisioning** – When a new zone is created using a template, all the records from the template are automatically added, reducing manual configuration efforts.
- **Consistency Across Zones** – Ensures uniformity in DNS configurations by enforcing a predefined structure for all newly created zones.
- **Time-Saving Management** – Eliminates repetitive manual entry of common records, speeding up DNS deployment.
- **Customizable Templates** – Administrators can create multiple templates to suit different use cases, such as internal zones, customer-specific setups, or service-specific configurations.

Usage Workflow

- **Create a Template:**
- Define a new zone template.
- Add default records that should be included in zones created from this template.
- **Apply the Template to a New Zone:**
- When creating a new DNS zone, select a predefined template.
- The system automatically applies the template's records to the new zone.

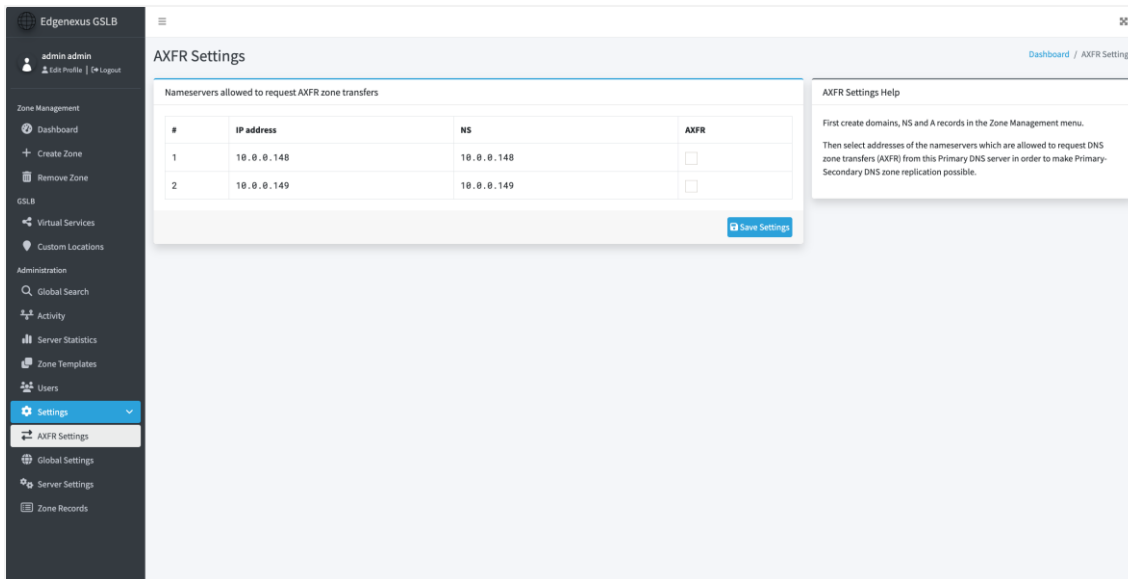
Modify and Manage Templates

Templates can be updated as needed, but changes do not affect previously created zones.

This feature enhances DNS management efficiency in EdgeGSLB Admin, particularly for environments requiring rapid and standardized zone deployment.

Settings

AXFR Settings



AXFR (Authoritative Zone Transfer) is a mechanism used in EdgeGSLB to transfer entire DNS zones from a primary name server to secondary name servers. This allows secondary servers to synchronize their records with the primary server, ensuring consistency and reliability in DNS resolution.

Overview of AXFR in EdgeGSLB

- AXFR (Asynchronous Full Zone Transfer) is primarily used in authoritative DNS servers to:
- Synchronize DNS zones between a primary (master) and secondary (slave) name server.
- Maintain redundancy and high availability by replicating zone data.
- Ensure that secondary servers receive updates when zone changes occur.

AXFR is a TCP-based transfer mechanism and is different from IXFR (Incremental Zone Transfer), which only transfers changes instead of the full zone.

How AXFR Works in EdgeGSLB

Below is a step-by-step breakdown of how an AXFR transfer occurs:

Scenario: Primary Server (Master) Transfers a Zone to a Secondary Server (Slave)

Primary Server Setup:

- EdgeGSLB is configured as a master (master=yes).
- AXFR is allowed only for specific secondary servers (allow-axfr-ips).
- NOTIFY messages are sent to secondary servers (also-notify).

Secondary Server Setup:

- EdgeGSLB is configured as a slave (slave=yes).
- The server listens for NOTIFY messages (allow-notify-from is set).
- The secondary server requests an AXFR when notified.

Zone Transfer Process:

- When a zone update occurs, the primary sends a NOTIFY message.
- The secondary receives the notification and checks the SOA (Start of Authority) record.

- If the SOA serial number is higher on the primary, the secondary requests an AXFR.
- The primary sends the full zone data over TCP.
- The secondary updates its zone file and serves updated DNS responses.

Global Settings

The Global Settings page in the GSLB UI allows the enablement of GSLB as a whole, and the enabling of Proxy Protocol.

The screenshot shows the EdgeGSLB Global Settings page. On the left is a sidebar with navigation options: Zone Management (Dashboard, Create Zone, Remove Zone), GSLB (Virtual Services, Custom Locations), and Administration (Global Search, Activity, Server Statistics, Zone Templates, Users, Settings). The main content area is titled 'Global Settings' and contains a 'Settings Editor' table. The table has three columns: 'Setting Name', 'Current Value', and 'Action'. It lists two settings: 'GSLB' (Current Value: On, Action: Turn Off) and 'PROXY Protocol' (Current Value: Off, Action: Turn On). To the right of the table is a 'Global Settings Help' section. It contains a 'GSLB' section explaining that GSLB requires zone record TTL set to 0 and zone cache disabled, and lists automatically applied parameter values: `cache-ttl=0`, `query-cache-ttl=0`, and `zone-cache-refresh-interval=0`. It also contains a 'PROXY Protocol' section explaining that GSLB requires an External IP defined for the GSLB app in the ADC host to learn DNS client IP addresses for location-based load-balancing. When the PROXY protocol is enabled, the GSLB app can run without an External IP and learn DNS client IP addresses from the PROXY header.

Setting Name	Current Value	Action
GSLB	On	Turn Off
PROXY Protocol	Off	Turn On

What is Proxy Protocol?

GSLB requires an External IP defined for GSLB app in the ADC host in order to be able to learn DNS client IP addresses for being able to implement location-based load-balancing, i.e. to respond to a DNS client with an IP address of a server, which is the geographically closest to the client.

When PROXY protocol is enabled, GSLB app is able to run without an External IP. The GSLB app can learn DNS client IP addresses from the PROXY header supplied by the ADC, which is hosting the app.

Please make sure to have PROXY protocol setting in sync with the ADC PROXY protocol setting, as it can't be detected automatically.

Server Settings

Name	Value	Edit
axfr-fetch-timeout	10	
cache-ttl	0	
carbon-interval	30	
default-ttl	3600	
distributor-threads	10	
dnssec-key-cache-ttl	30	
log-dns-details	Off	
log-dns-queries	Off	
loglevel	4	
max-cache-entries	1000000	

There are a number of settings that you can adjust on the EdgeGSLB. Changing values here and applying them, makes changes to the underlying PowerDNS server.

Clicking on any of the settings will take you to the relevant PowerDNS server documentation section. For example, clicking on the 'axfr-fetch-timeout' parameter will show the following.

axfr-fetch-timeout

- Integer
- Default: 10

New in version 4.3.0.

Maximum time in seconds for inbound AXFR to start or be idle after starting.

Logging and Log Levels

One of the most important requirements of system and security administrators is the ability to glean logs and save them for analysis. The EdgeGSLB provides this facility within the Server Settings area, allowing the enablement of logging as well as the setting of logging levels.

Loglevel Description

Log Level	Description
0	No logging. All log messages are suppressed.
1	Critical messages only. Logs only critical issues that require immediate attention.
2	Errors. Logs error conditions that might allow the server to continue running.
3	Warnings. Logs warning messages about potential issues that are non-critical.
4	Notices. Logs normal but significant conditions.
5	Informational messages. Logs general informational messages about server operations.

6	Debug messages. Logs detailed debugging information for troubleshooting.
7-9	Increasingly verbose debug messages. Higher values provide more granular debug information.

Logs created within the EdgeGSLB are stored locally for a short period and then added to the general system log of the ADC.

Zone Settings

This page allows you to select the type of zone record that will be available in the Forward and Reverse-Lookup zones.

The screenshot shows the 'Zone Record Settings' page in the EdgeGSLB administrator interface. The left sidebar contains navigation links for Zone Management, GSLB, Administration, and Settings. The main content area is titled 'Zone Record Settings' and features a 'Settings Editor' tab. Below the tab is a table with 16 rows, each representing a DNS record type. The table has columns for '#', 'Record', 'Forward Zone', and 'Reverse Zone'. Checkmarks are present in the 'Forward Zone' and 'Reverse Zone' columns for records 1 (NS), 2 (A), 4 (LOC), 8 (CAA), 11 (AAAA), and 16 (CERT). A 'Settings Editor Help' box is visible on the right, containing text about selecting record types and a link to PowerDNS docs.

#	Record	Forward Zone	Reverse Zone
1	NS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	A	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	URI	<input type="checkbox"/>	<input type="checkbox"/>
4	LOC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	CDNSKEY	<input type="checkbox"/>	<input type="checkbox"/>
6	KEY	<input type="checkbox"/>	<input type="checkbox"/>
7	RP	<input type="checkbox"/>	<input type="checkbox"/>
8	CAA	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9	AFSDB	<input type="checkbox"/>	<input type="checkbox"/>
10	SMIMEA	<input type="checkbox"/>	<input type="checkbox"/>
11	AAAA	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12	TKEY	<input type="checkbox"/>	<input type="checkbox"/>
13	NSEC3PARAM	<input type="checkbox"/>	<input type="checkbox"/>
14	SSHFP	<input type="checkbox"/>	<input type="checkbox"/>
15	LUA	<input type="checkbox"/>	<input type="checkbox"/>
16	CERT	<input type="checkbox"/>	<input type="checkbox"/>

You can also check the PowerDNS page here:
<https://doc.powerdns.com/authoritative/appendices/types.html>