Progress®
Kemp® LoadMaster®

Feature Description GEO

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 6

Document Purpose 7

Intended Audience 7

Chapter 2: Benefits of GEO 8

Speed 8

Scalability 8

Manageability 9

Chapter 3: GEO Examples 10

How GEO Typically Works 10

On-prem to On-prem 11

Hybrid Cloud (Azure or AWS) 13

GSLB Only 14

Horizontal Scale (Multiple GEO LoadMasters in Each Site) 14

GEO Answer to a DNS Query A or AAAA 16

DNSSEC Examples 21

Chapter 4: Deploying GEO 26

GEO Best Practices 27

Enable/Disable GEO 27

GEO Homepage 28

Login Information 28

General Information 28

WAF Status 29

System Metrics 29
License Information 29
About LoadMaster 29
Other Links 30
GSLB Menu Options 31
Specify what Interfaces to Use for GEO Responses and Requests 33
Enable Alternate Gateway Support 33
DNS Responder 33
Client Source IP 35
DNS Integration/Delegation 38
GEO Miscellaneous Params 45
Zone 45
Source of Authority 46
Global 47
Resource Check Parameters 49
Stickiness 49
Location Data Update 50
GEO System Info / Debug 50
Fully Qualified Domain Name (FQDN) 53
FQDN Filtering and Sorting 53
Add an FQDN 54
FQDN Health Check Options 57
Scheduling Methods 60
Additional Records 64
IP Range Selection Criteria 65
Unanimous Cluster Health Checks 67
Manage Clusters 68
Cluster Types 69
Real Server/Cluster Health Checking 70
Add a Cluster 72
Connect a LoadMaster to a GEO LoadMaster 73
Add the FQDN and the Virtual Service IP Address 73
Modify a Cluster 74

Delete a Cluster 75
Clustering Configuration Advice 76
Configure DNSSEC 76
GSLB Statistics 79
Remote Administration 80
IP Access List Settings 80
Certificates 82
Distributed LoadMaster Partners 82
HA Versus Partners 83
Set Up GEO LoadMaster Partners 84
Upgrading GEO Partners 87
Configuring GEO for Exchange Site Resiliency 87
Enabling Fail Over 88
Delaying a Failover 88
Requiring Manual Intervention Before Failback Occurs 89
Configuring Site Resiliency Options for Exchange (Example Configuration) 90

Chapter 5: Troubleshooting 92
Persistence/Stickiness 92
Scheduling 93

Chapter 6: References 95

1

Introduction

GEO offers the ability to move past the single data center, allowing for multi data center High Availability (HA). Even when a primary site is down, traffic is directed to the disaster recovery site. Also included in GEO is the ability to ensure clients connect to their fastest performing and geographically closest data center.

The GEO product is available in two forms:

- A standalone GEO product
- A Global Server Load Balancing (GSLB) Feature Pack that is part of the Progress Kemp load balancer (LoadMaster) product

Note: Throughout this document, when we refer to the "GEO LoadMaster" we are referring to **either** the GEO LoadMaster or the LoadMaster with the GSLB Feature Pack enabled.

GEO has the same management interfaces as the LoadMaster appliances, including all the foundation technology such as syslog logging, email notifications, interface bonding, and Gigabit support. GEO provides advanced application health checking, to ensure that unavailable services or data centers are not visible to clients. Health checking occurs at the site level, allowing for flexible decision making on when traffic should be diverted per Fully Qualified Domain Name (FQDN).

GEO can be deployed in a distributed (active/active) high availability configuration, with multiple GEO LoadMasters securely synchronizing information. Introducing GEO into existing Authoritative Domain Name Services (DNS) requires minimal integration work and risk, allowing you to fully leverage the existing DNS investment.

GEO securely and seamlessly integrates with core LoadMaster functionality to offer **Real Server Load** balancing, in which GEO uses local data center metrics provided by the LoadMaster, allowing clients to connect to the most available target. This is supported in both the GSLB feature pack and the standalone

GEO product.

GEO handles A (IPv4) and AAAA (IPv6) records. As of LoadMaster firmware version 7.2.53, a new **Additional Records** section has been added to configure records for a specific FQDN. You can add, modify, or delete additional TXT, CNAME, and MX records to/from an FQDN.

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience

Document Purpose

The purpose of this document is to give an overview of the GEO product and its functionality.

Intended Audience

This document is intended to be read by anyone who is interested in finding out more about Progress Kemp's GEO product.

2

Benefits of GEO

There are a number of benefits to using GEO including speed, scalability, and manageability. For more information, refer to the sections below.

Related Links

For details, see the following topics:

- Speed
- Scalability
- Manageability

Speed

GEO ensures that mission-critical servers are continuously available and performing reliably. GEO can monitor server and application load. This information is then used to intelligently direct user requests to the cluster that is most available. By intelligently redirecting traffic, the LoadMaster eliminates server overload conditions and round trip propagation delays that may slow performance, allowing you to increasing end-user application speed.

Scalability

GEO solves the scalability dilemma in the common adage: “Growth is the challenge, scalability is the key”.

GEO solves this by continuing to support increasing network server workloads and still providing high reliability. GEO:

- Intelligently distributes traffic across server arrays or data centers
- Reduces the need for increasingly larger and more expensive servers to accommodate increases in network traffic
- Enables many distributed application servers to function as a single, virtual server
- Reduces the risks of all application resources deployed at a single geographical location
- Allows for the orderly addition of new resources, or routine data center maintenance without disrupting service to the end user
- Can be used with multiple heterogeneous hardware platforms allowing organizations to protect their investments in their legacy hardware installations, as well as integrate future hardware investments

Manageability

GEO is easy to set up, and easy to manage. Network management is made easy, administrators can deploy new servers and take individual data centers offline for routine maintenance without disrupting services to end-users. Integrating GEO into an existing DNS infrastructure can be done with no service impact and allows for distributed administration.

3

GEO Examples

Refer to the sections below for some examples of how GEO works.

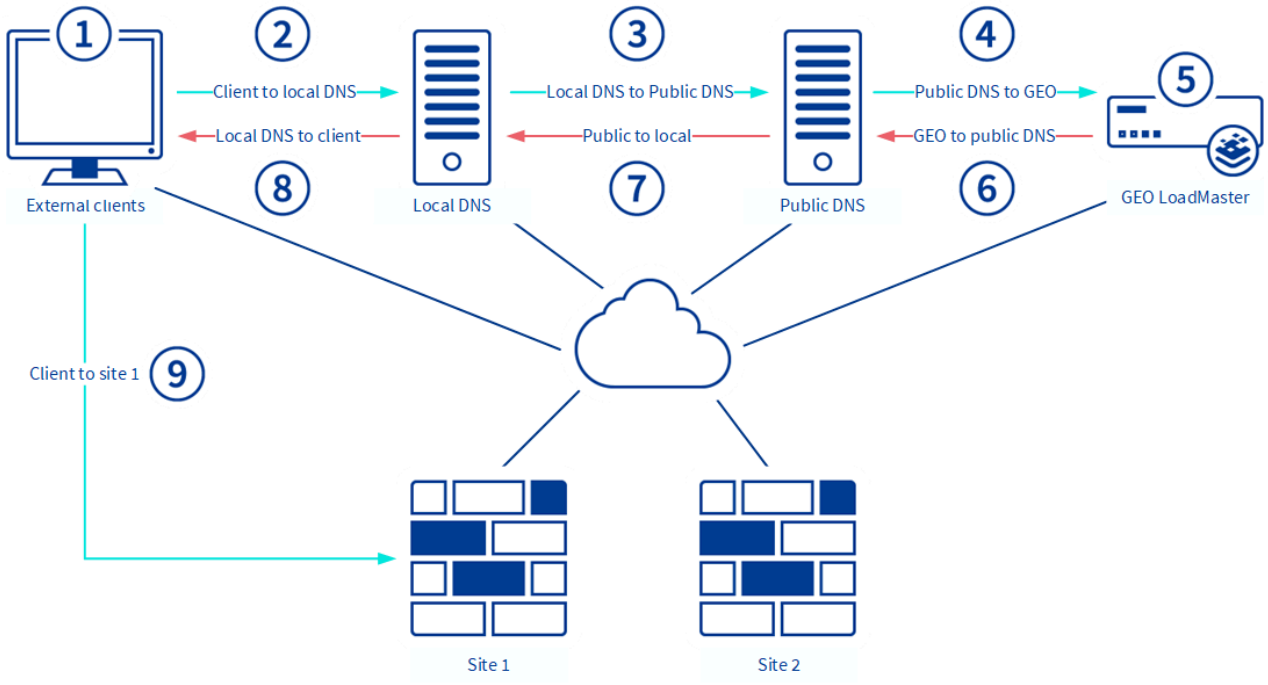
Related Links

For details, see the following topics:

- How GEO Typically Works
- GEO Answer to a DNS Query A or AAAA
- DNSSEC Examples

How GEO Typically Works

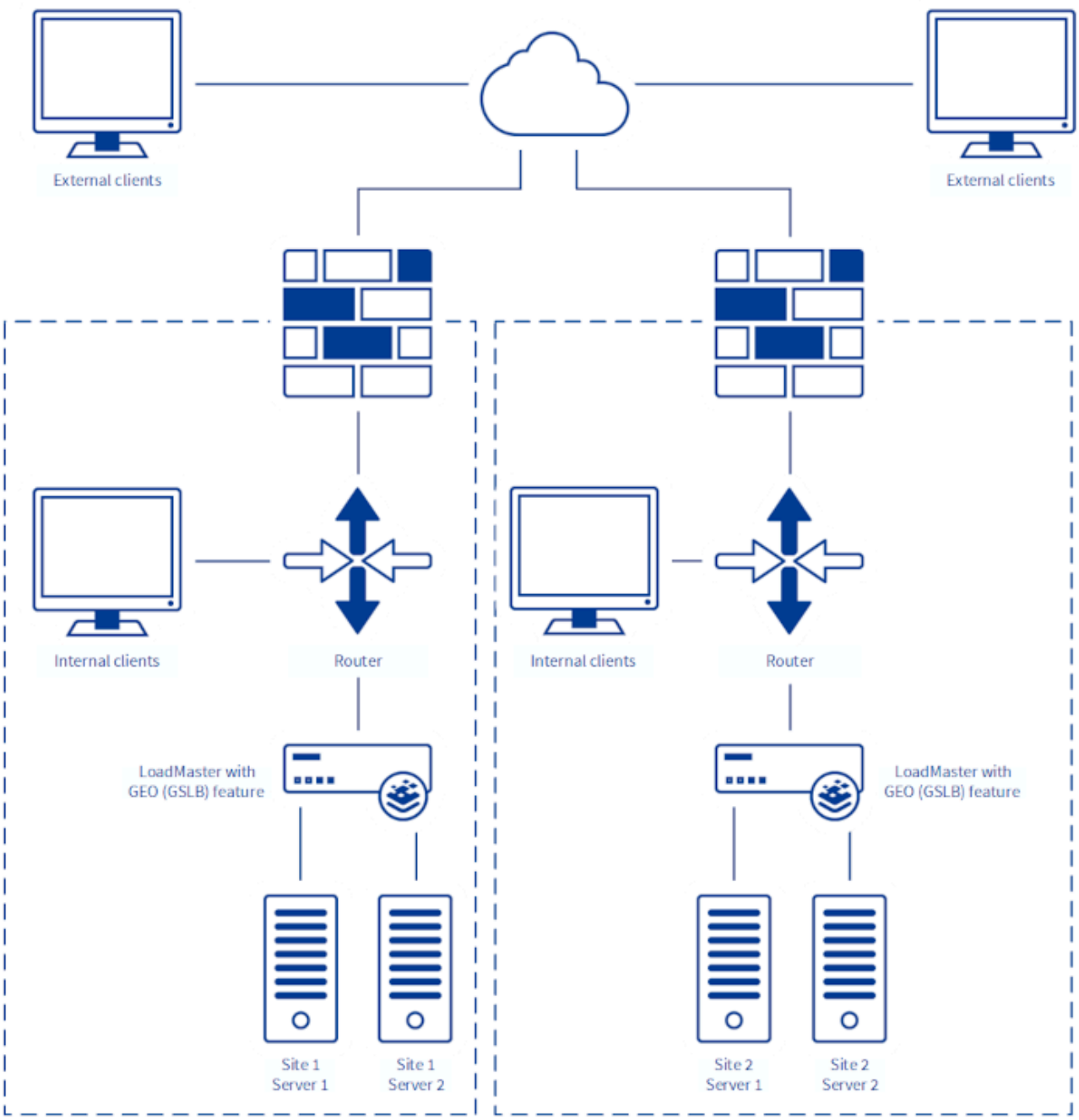
This section describes how the GEO functionality typically works. Please note that within this configuration we are depicting the GEO LoadMaster as being located outside the data centers to make the flow clear. Though this can be the case, typically the GEO LoadMaster would be located within one or more of the data centers.



1. A public client tries to connect to FQDN **test.domain.com**.
2. The public client checks its local DNS.
3. The local DNS forwards the request to the public DNS.
4. The Public DNS forwards the request to GEO as it is the authoritative DNS for this record.
5. GEO checks persistence and scheduling and decides which site to return.
6. GEO returns the IP address for the client that made the request (in this case; the public DNS).
7. The public DNS returns the results to the Local DNS.
8. The local DNS returns the result to the client.
9. The client connects directly to the site.

On-prem to On-prem

Refer to the network diagram below for an example on-prem to on-prem scenario.

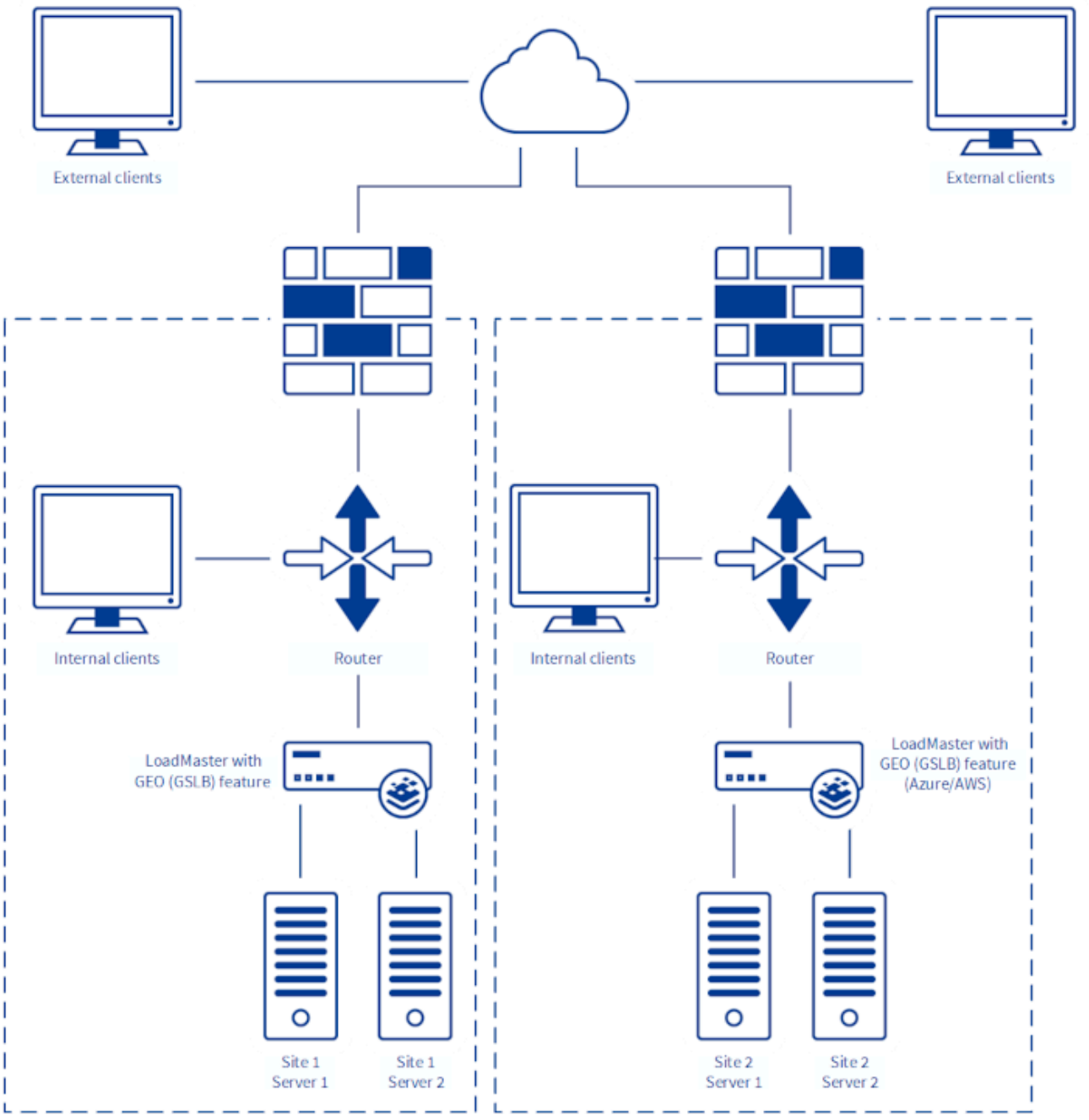


The above diagram could apply to the following setups (depending on the GEO configuration and your environment/topology):

- Active/Active site setup
- Active/Disaster Recovery (DR) site setup
- GEO location/proximity scheduling method setup

Hybrid Cloud (Azure or AWS)

Refer to the network diagram below for an example hybrid cloud (Azure or AWS) scenario.

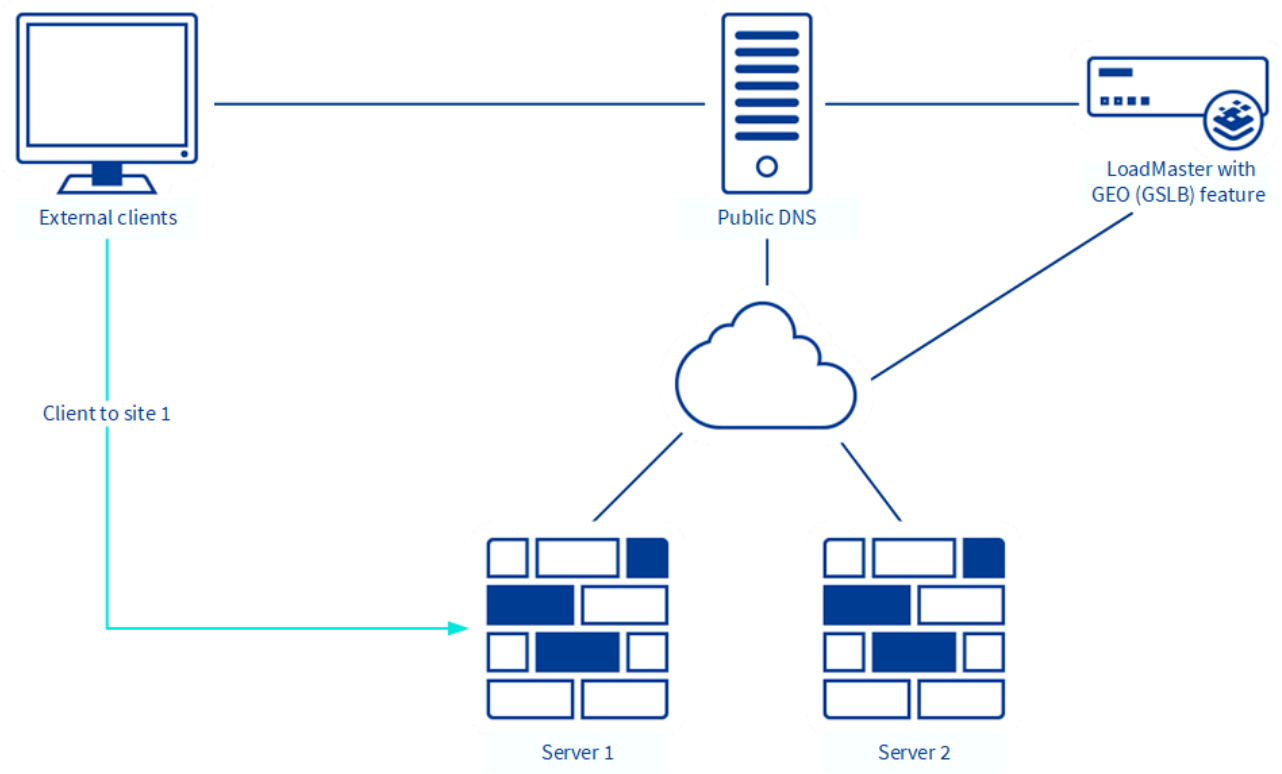


The above diagram could apply to the following setups (depending on the GEO configuration and your environment/topology) where the secondary site is in the cloud:

- Active/Active site setup
- Active/Disaster Recovery (DR) site setup
- GEO location/proximity scheduling method setup

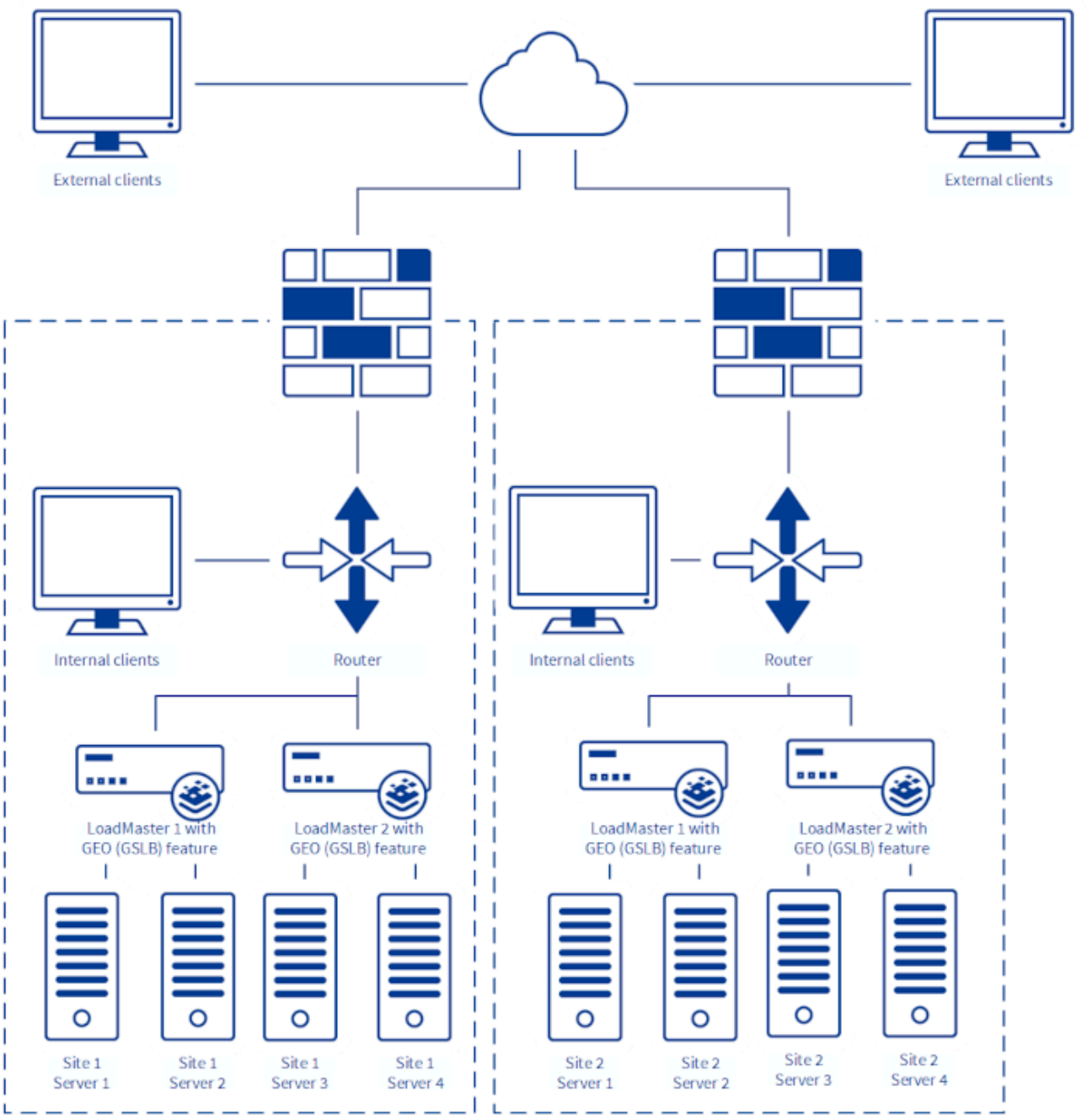
GSLB Only

Refer to the network diagram below for an example Global Server Load Balancing (GSLB) only scenario.



Horizontal Scale (Multiple GEO LoadMasters in Each Site)

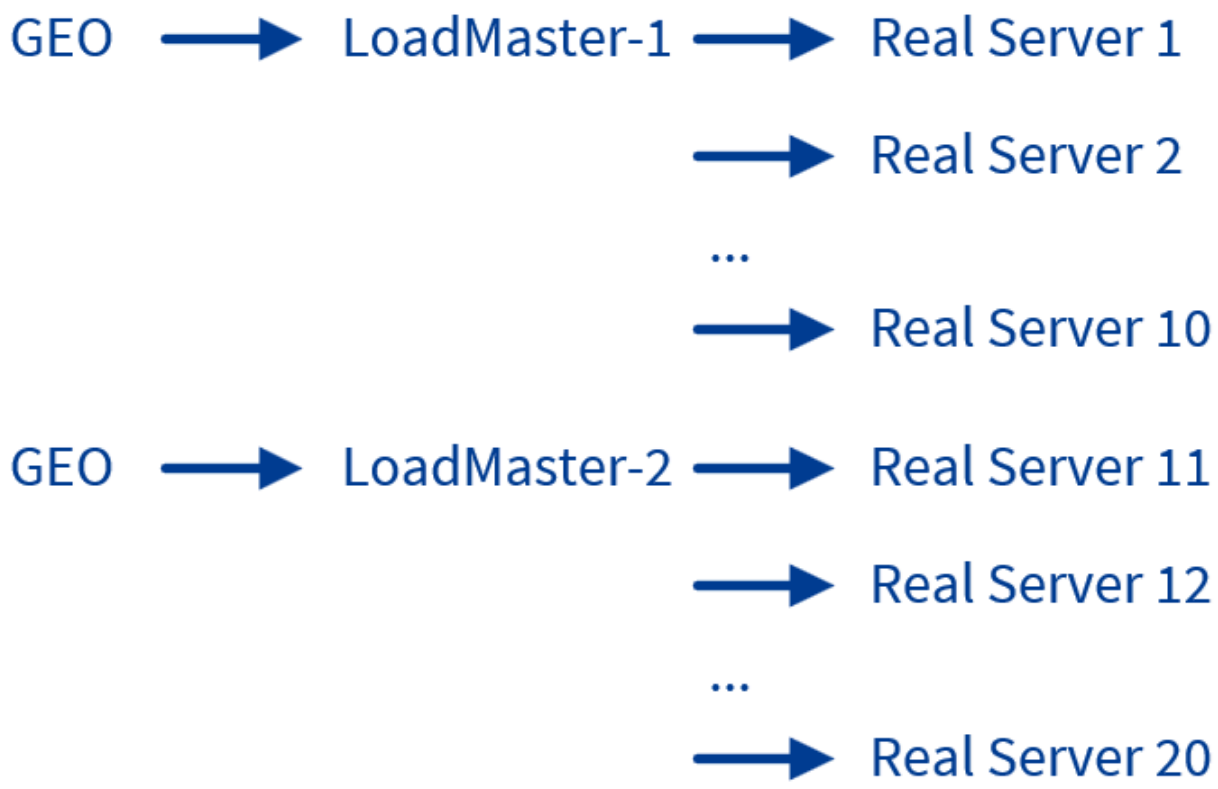
Refer to the network diagram below for an example horizontal scale (multiple GEO LoadMasters in each site) scenario.



In this type of scenario:

- A client requests an answer for an FQDN.
- GEO round-robins between multiple LoadMasters.
- The LoadMaster also round-robins between multiple Real Servers.

For example:



GEO Answer to a DNS Query A or AAAA

This section provides examples of how GEO responds to various DNS requests from clients. These examples assume that DNSSEC is not enabled; see the next section for DNSSEC-related examples.

When a query runs against GEO, GEO gets the IP address of the client. The client could have a public IP or a private IP (meaning the client is in the same network as GEO).

Examples of private IP address ranges are provided in the table below:

Range	Network type
10.0.0.0 – 10.255.255.255	Class A network
172.16.0.0 – 172.31.255.255	Class B networks
192.168.0.0 – 192.168.255.255	Class C networks

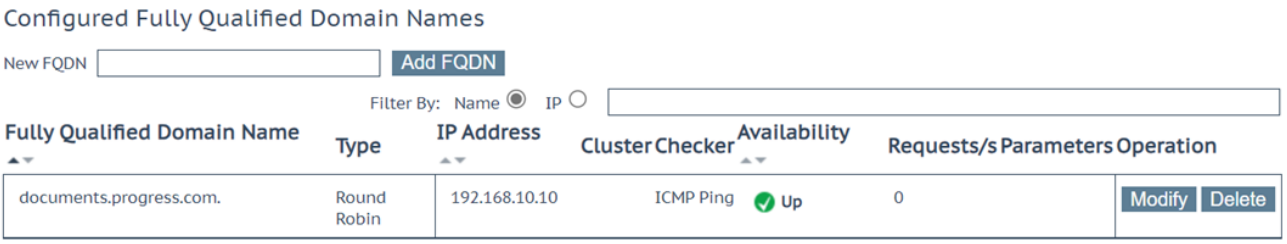
The **Public Requests** and **Private Requests** drop-downs in the modify FQDN screen allows granular control of DNS responses. This provides finer control of DNS responses to configured FQDNs. Administrators may selectively respond with public or private sites based on whether the client is from a public or private IP. For example, administrators may wish to allow only private clients to be sent to private sites. For a table breaking down what site types are allowed depending on the client IP address type and the Public/Private Requests setting, refer to the Add an FQDN section.

For the examples in this section, we will assume the following settings in GEO:



Case 1: If the FQDN has a site defined in GEO, it answers with the configured site IP address.

In this case, the FQDN in the **dig** query below (**documents.progress.com**) is configured in the GEO configuration:



So, GEO responds with the configured IP address in a DNS response that looks like the example below:

Dig example

```
$ dig A documents.progress.com @192.168.1.154


;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44482

;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; WARNING: recursion requested but not available


;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

;; QUESTION SECTION:
```

```
;documents.progress.com.      IN      A


;; ANSWER SECTION:

documents.progress.com. 10    IN      A       192.168.10.10


;; AUTHORITY SECTION:

documents.progress.com.    10      IN      NS      geo.progress.com.


;; Query time: 2 msec

;; SERVER: 192.168.1.154#53(192.168.1.154)

;; WHEN: Fri May 24 08:31:40 IST 2024

;; MSG SIZE  rcvd: 113
```

nslookup example

```
nslookup -q=a documents.progress.com 192.168.1.154

Server: UnKnown

Address: 192.168.1.154

Name: documents.progress.com

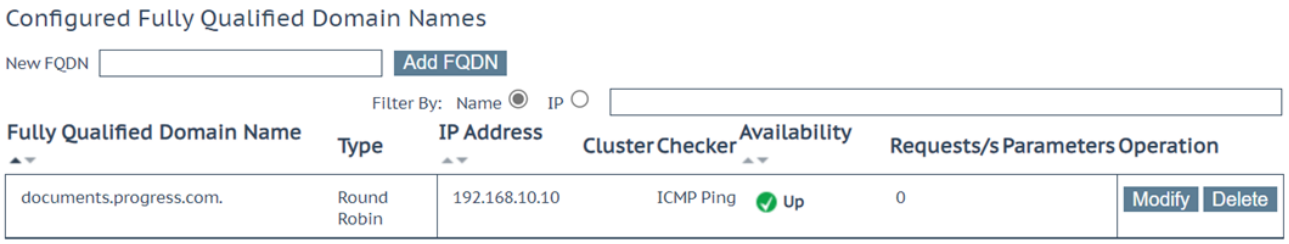
Address: 192.168.10.10
```

Case 2: GEO is aware of the FQDN but no endpoint is available.

The answer from GEO will be NOERROR and will follow the general format shown below. The content of the authority section depends on whether the FQDN is defined on GEO:

- If the FQDN is defined on GEO, this section contains the SOA (Start of Authority) record from GEO's configuration.
- If the FQDN is defined in another zone that GEO knows about but is defined on another DNS server, the authority section in the response includes the SOA information GEO obtained from the authoritative DNS server for the domain.

The following is how an FQDN that was created but no IP address was assigned looks in the GEO UI:



The example below shows what GEO response to a query for the above FQDN would look like.

Dig example

```
$ dig A documents.progress.com @192.168.1.154

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39220

;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; WARNING: recursion requested but not available



;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

;; QUESTION SECTION:

;documents.progress.com.      IN      A



;; AUTHORITY SECTION:

documents.progress.com.    10      IN      SOA     SOA progress.com.
admin\@progress.com. 149 86400 7200 2419200 10



;; Query time: 1 msec

;; SERVER: 192.168.1.154#53(192.168.1.154)

;; WHEN: Fri May 24 08:36:07 IST 2024
```

```
;; MSG SIZE  rcvd: 133
```

nslookup example

```
nslookup -q=a documents.progress.com 192.168.1.154

Server:  UnKnown

Address:  192.168.1.154

Name:    documents.progress.com
```

Case 3: The FQDN does not exist

In this case, the FQDN does not exist in the GEO configuration, nor in the configuration of any DNS server with which GEO is communicating.

The response is REFUSED and will look like the example below.

Dig example

```
$ dig A nondocuments.progress.com @192.168.1.154


;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 21740

;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; WARNING: recursion requested but not available


;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

;; QUESTION SECTION:

;nondocuments.progress.com.          IN      A
```

```
;; Query time: 1 msec

;; SERVER: 192.168.1.154#53(192.168.1.154)

;; WHEN: Fri May 24 08:38:33 IST 2024

;; MSG SIZE  rcvd: 82
```

nslookup example

```
nslookup -q=a nondocuments.progress.com 192.168.1.154

Server:  UnKnown

Address:  192.168.1.154

*** UnKnown can't find nondocuments.progress.com: Query refused
```

DNSSEC Examples

DNSSEC only works when a zone name is defined and it only works for the FQDNs that belong to the zone. FQDNs that do not belong to a defined zone will provide an answer without the DNSSEC signature.

Case 1: FQDN does not belong to a Zone Name

```
$ dig A foo.example.com +dnssec @3.83.34.12


; <<>> DiG 9.10.3-P4-Ubuntu <<>> A foo.example.com +dnssec @3.83.34.12

;; global options: +cmd

,

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24329

;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; WARNING: recursion requested but not available


;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags: do; udp: 4096

;; QUESTION SECTION:

;foo.example.com.               IN      A


;; ANSWER SECTION:

foo.example.com.        10      IN      A       1.1.1.1


;; AUTHORITY SECTION:

foo.example.com.        10      IN      NS      soa.ZoneNameExample.com.


;; Query time: 224 msec

;; SERVER: 3.83.34.12#53(3.83.34.12)

;; WHEN: Tue Oct 08 11:15:51 IST 2019

;; MSG SIZE  rcvd: 94
```

Case 2: FQDN belongs to a Zone Name

```
$ dig A fqdn.ZoneNameExample.com +dnssec @3.83.34.12


; <<>> DiG 9.10.3-P4-Ubuntu <<>> A fqdn.ZoneNameExample.com +dnssec @3.83.34.12

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25994

;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags: do; udp: 4096

;; QUESTION SECTION:

;fqdn.ZoneNameExample.com.      IN      A



;; ANSWER SECTION:

fqdn.ZoneNameExample.com. 10    IN      A       1.1.1.1

fqdn.ZoneNameExample.com. 10    IN      RRSIG   A 8 3 10 20191107054647
20191008044647 22641 zonenameexample.com. ZnBg0vsjOLK37x5ZH3o82o8Id5nCBT/
IFP2rQTajtjF/zOV4UHHp5KBs
7CDFdFkyfyQ1vT3ZFyXaxFJ1GcxmOizzkgfwP4CqOdwQwMzWbvk9dlQ+
M33drzO7MzGQjQS3Mg8ptow9FLoNY3unc8+KgDJGxhJzIHY+okzJITZN cvM=



;; AUTHORITY SECTION:

ZoneNameExample.com.    10      IN      NS      soa.ZoneNameExample.com.

ZoneNameExample.com.    10      IN      RRSIG   NS 8 2 10 20191107050733
20191008044631 22641 zonenameexample.com. N0QLBBM55+TCVCQfk4cbYk5IY7L3jgp7O/
Dv4yss1dqlO4z4EGhwbqul jsr4BzhZzqYnJvsZaTl+roEKdJAS8fgx24uXQpeDsBjiukJYsR5ZjDuT
fhGnf9By7CdkEWr4rdU+Q7eDPmdigXWDvru2K6ui8Inzy1kEkCB5zYhU YJ8=



;; ADDITIONAL SECTION:

soa.ZoneNameExample.com. 10     IN      A       172.16.1.192

soa.ZoneNameExample.com. 10     IN      RRSIG   A 8 3 10 20191107050733
20191008044631 22641 zonenameexample.com. N0RW69lu/7IWPY/
Z9DufZlZuDVE0KmY8AgzLvo1JneicHF27wElKKVUa
0lSVD15yypeSD96T0hZIkqVhKrgv43UKTYu3khR7I+wl53gYie3qaLnA 0HmBG/
GD1tmW8Pky7B7hCGz7DbpI+fqenZHzyCGdu7alYy0PhoQNcFRZ xlA=



;; Query time: 229 msec

;; SERVER: 3.83.34.12#53(3.83.34.12)

;; WHEN: Tue Oct 08 11:17:19 IST 2019
```

```
;; MSG SIZE  rcvd: 640
```

Case 3: Zone name defined, FQDN that belongs to the zone but is not defined in GEO

In this case, GEO answers **NXDOMAIN**.

```
dig @172.16.0.65 A notexisting.fab.com



; <<>> DiG 9.11.4-P2-RedHat-9.11.4-3.P2.fc27 <<>> @172.16.0.65 A
notexisting.fab.com

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 44488

;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; WARNING: recursion requested but not available



;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;notexisting.fab.com.   IN A



;; AUTHORITY SECTION:

fab.com.  10 IN SOA nameserver.fab.com. hostmaster.fab.com. 29 86400 7200
2419200 10



;; Query time: 1 msec

;; SERVER: 172.16.0.65#53(172.16.0.65)

;; WHEN: Tue Oct 08 08:32:16 EDT 2019
```

```
;; MSG SIZE  rcvd: 97
```

4

Deploying GEO

The sections below refer to various aspects of GEO deployment.

Related Links

For details, see the following topics:

- GEO Best Practices
- Enable/Disable GEO
- GEO Homepage
- Login Information
- GSLB Menu Options
- Specify what Interfaces to Use for GEO Responses and Requests
- Enable Alternate Gateway Support
- DNS Responder
- Client Source IP
- DNS Integration/Delegation
- GEO Miscellaneous Params
- GEO System Info / Debug
- Fully Qualified Domain Name (FQDN)

- IP Range Selection Criteria
- Unanimous Cluster Health Checks
- Manage Clusters
- Configure DNSSEC
- GSLB Statistics
- Remote Administration
- IP Access List Settings
- Certificates
- Distributed LoadMaster Partners
- Configuring GEO for Exchange Site Resiliency
- Enabling Fail Over
- Delaying a Failover
- Requiring Manual Intervention Before Failback Occurs
- Configuring Site Resiliency Options for Exchange (Example Configuration)

GEO Best Practices

Some best practices relating to LoadMaster GEO deployments are as follows:

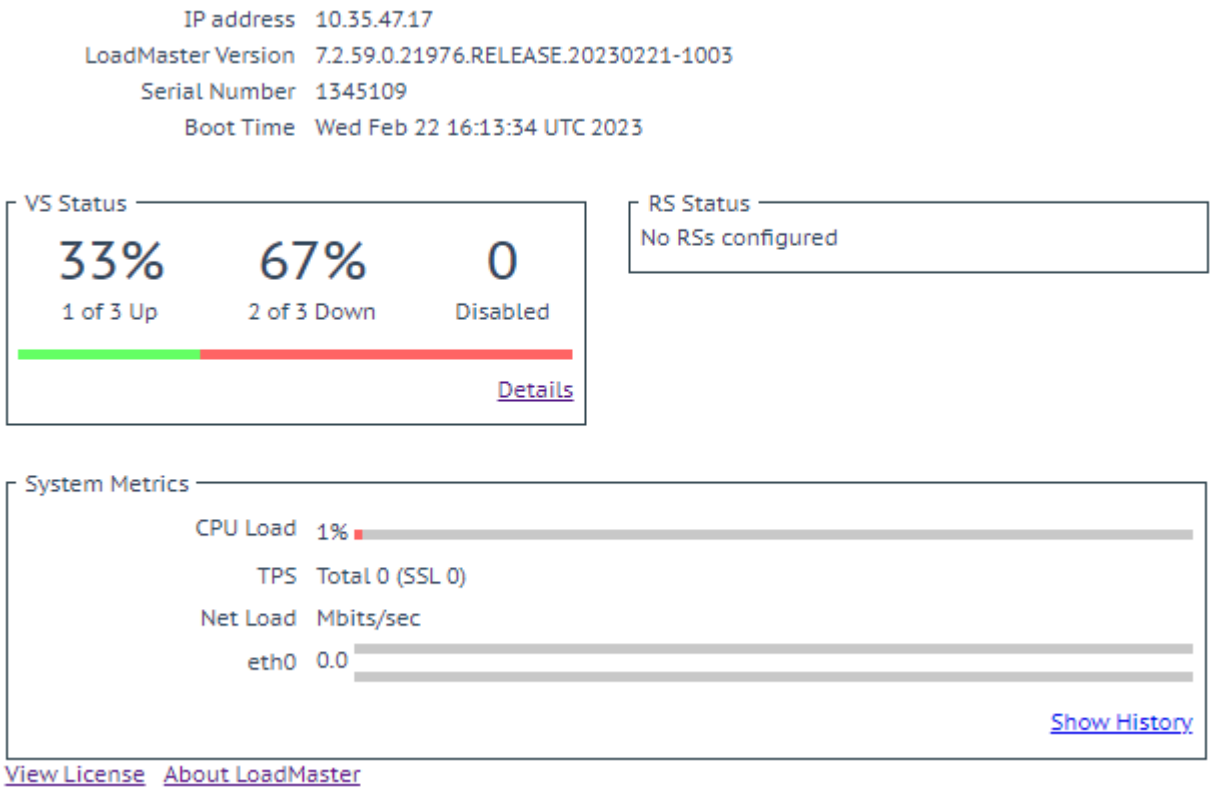
- Ensure you are using the latest Generally Available (GA) or Long Term Support Feature (LTSF) LoadMaster firmware.
- Ensure you are using the latest GEO location database. For further details on how to update this, refer to the following section: Location Data Update.
- Ensure you have a backup policy in place. For further details, refer to the **Backup and Restore, Technical Note**.

Enable/Disable GEO

When using the GSLB Feature Pack, GEO can be enabled or disabled by clicking either the **Enable GSLB** or **Disable GSLB** menu option under **Global Balancing** in the main menu of the LoadMaster WUI. When GSLB capabilities are enabled on a LoadMaster, the **Packet Routing Filter** is also enabled and required. When GEO is disabled, it is possible to either enable or disable the **Packet Routing Filter** in **System Configuration > Access Control > Packet Filter**.

Note: **Disable GSLB** can be performed by any user with the **GEO Control** permission. **Enable GSLB** can only be performed by the **bal** user.

GEO Homepage



Refer to the sections below for a description of the different parts of the home screen.

Login Information

After initially logging in to the LoadMaster, if Session Management is enabled - some login information is displayed:

- The last login time and IP address of the current user
- The number of successful logins by the current user in the last 30 days
- The total number of failed login attempts by any user (including unknown usernames) since the last successful login

General Information

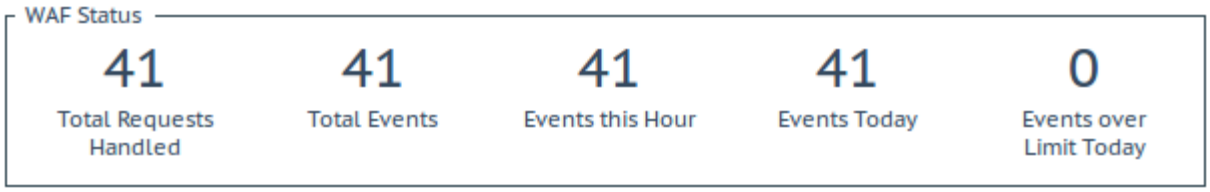
IP address: The IP address of the LoadMaster.

LoadMaster Version: The firmware version of the LoadMaster.

Serial Number: The Serial Number of the LoadMaster.

Boot Time: The time of the last server reboot.

WAF Status



The **WAF Status** section will only appear on WAF-capable LoadMasters. For further information on WAF, please refer to the Web Application Firewall, Feature Description.

System Metrics

CPU Load: The percentage of load to the CPU of the LoadMaster appliances and to the CPU running a Virtual LoadMaster (VLM).

TPS [conn/s]: The total number of Transactions Per Second and the number of Secure Sockets Layer (SSL) transactions per second.

WAF Stats: Web Application Firewall (WAF) status - shows the total number of handled connections, and the total number of incidents.

Net Load: Network load in megabits per second, shown for each configured interface.

CPU Temp.: Displays the temperature of the CPU.

The CPU Load and Net Load data is updated every 5 seconds.

License Information

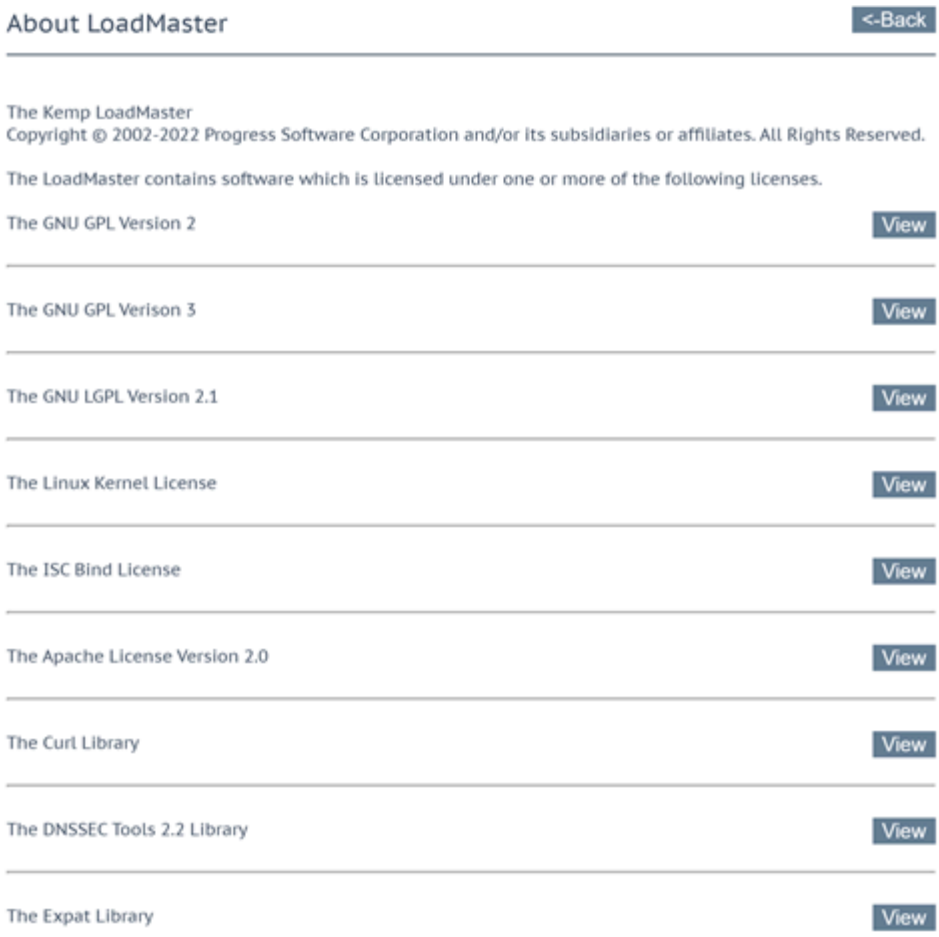
Clicking the **View License** link will display model, subscription, subscription expiry and subscription feature details, such as the activation date and end date of the LoadMaster license.

Note: If the subscription has expired, a message is displayed in the **License Information** section. To renew the subscription, please contact Progress Kemp.

Upgrade: Upgrade the LoadMaster by buying a license from the Progress Kemp purchase portal.

About LoadMaster

On the **About LoadMaster** page, you can view licenses for third party software that is used in the LoadMaster.



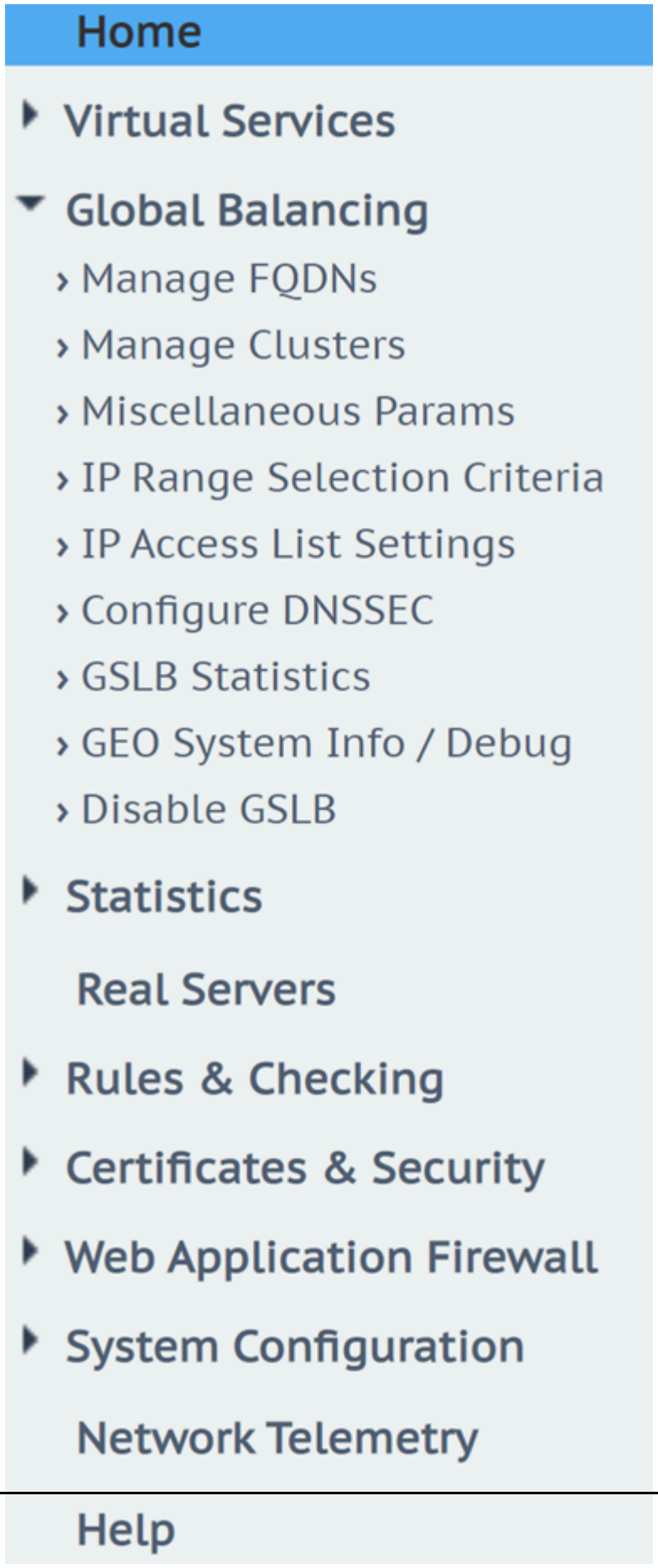
To view a license, click the **View** button next to the relevant item.

Other Links

Other links are provided at the bottom of the home page:

- **Support & FAQ:** A link to the Progress Kemp Support site
- **Find Online Documentation:** A link to the Progress Kemp documentation page

GSLB Menu Options


Home
Virtual Services
Global Balancing
› Manage FQDNs
› Manage Clusters
› Miscellaneous Params
› IP Range Selection Criteria
› IP Access List Settings
› Configure DNSSEC
› GSLB Statistics
› GEO System Info / Debug
› Disable GSLB
Statistics
Real Servers
Rules & Checking
Certificates & Security
Web Application Firewall
System Configuration
Network Telemetry
Help

When using the GSLB Feature Pack on a LoadMaster, the GEO-related options can be found by selecting the **Global Balancing** option in the main menu on the left of the WUI.

Specify what Interfaces to Use for GEO Responses and Requests

There is another GEO option which is not contained in the **Global Balancing** main menu option – **Use for GEO Responses and Requests**. You can get to this setting by going to **System Configuration > Network Setup** and selecting the relevant interface.

By default, only the default gateway interface is used to listen for and respond to DNS requests. This field gives you the option to listen on additional interfaces. When this option is enabled, GEO also listens on any **Additional addresses** that are configured for the interface.

Note: This option cannot be disabled on the interface containing the default gateway. By default, this is eth0.

Note: LoadMaster High Availability (HA) pairs only listen on the shared IP address.

Enable Alternate Gateway Support

If there is more than one interface enabled, there is an option which provides the ability to move the default gateway to a different interface.

Enabling this option adds another option to the **Interfaces** screen – **Use for Default Gateway**.

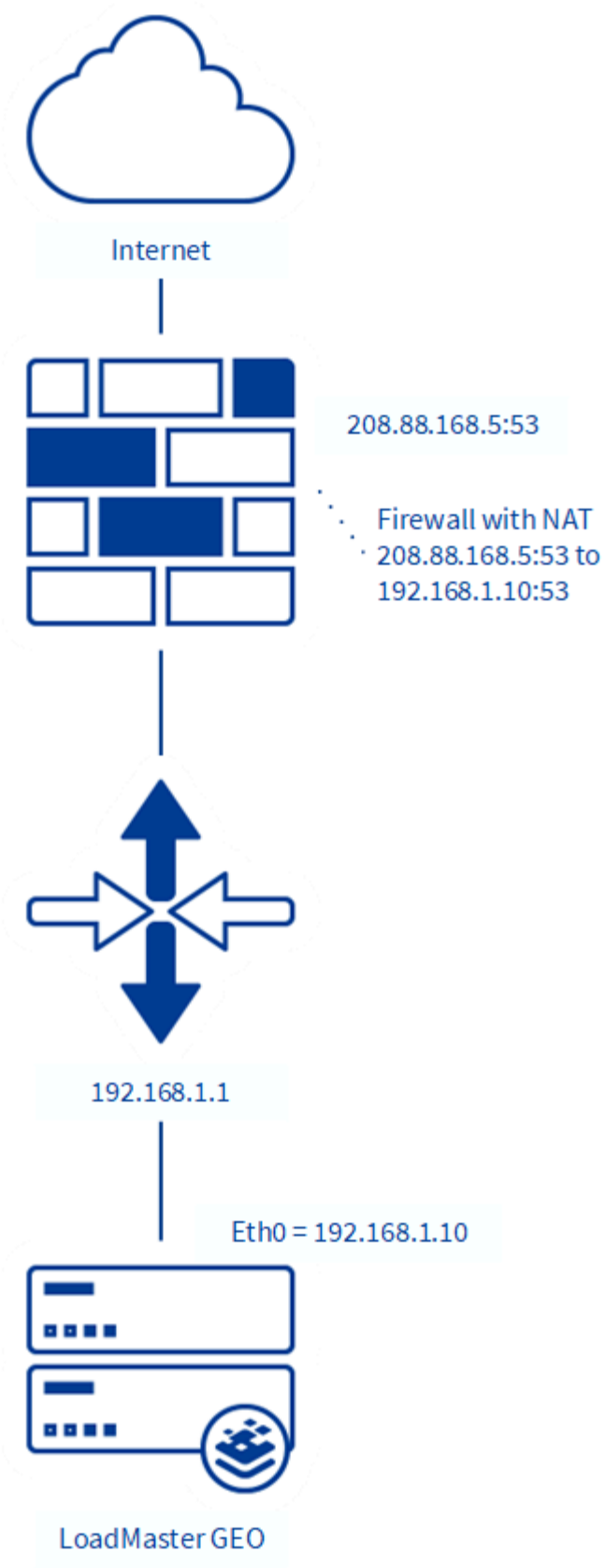
Note: The Enable Alternate GW support option will appear in **Certificates & Security > Remote Access** in GEO only LoadMasters.

Note: The **Enable Alternate GW support** option will appear in **System Configuration > Miscellaneous Options > Network Options** in LoadMaster + GEO products.

DNS Responder

LoadMaster connects to one or more networks. By default, a single interface (eth0) is used for DNS responses. In this documentation, eth0 is assumed to be used as the sole interface used for DNS responses.

In a one-armed configuration, the DNS responder service can be configured for any subnet. The LoadMaster connects to a Layer 2 network through a single interface, eth0.


Internet
208.88.168.5:53
Firewall with NAT
208.88.168.5:53 to
192.168.1.10:53
192.168.1.1
Eth0 = 192.168.1.10
LoadMaster GEO

If a firewall is already in place performing NAT to a DMZ in a non-routable (RFC1918) IP space (for example, 192.168.x.x or 10.x.x.x), please make sure a 1-to-1 NAT for port 53 UDP/TCP exists to the LoadMaster.

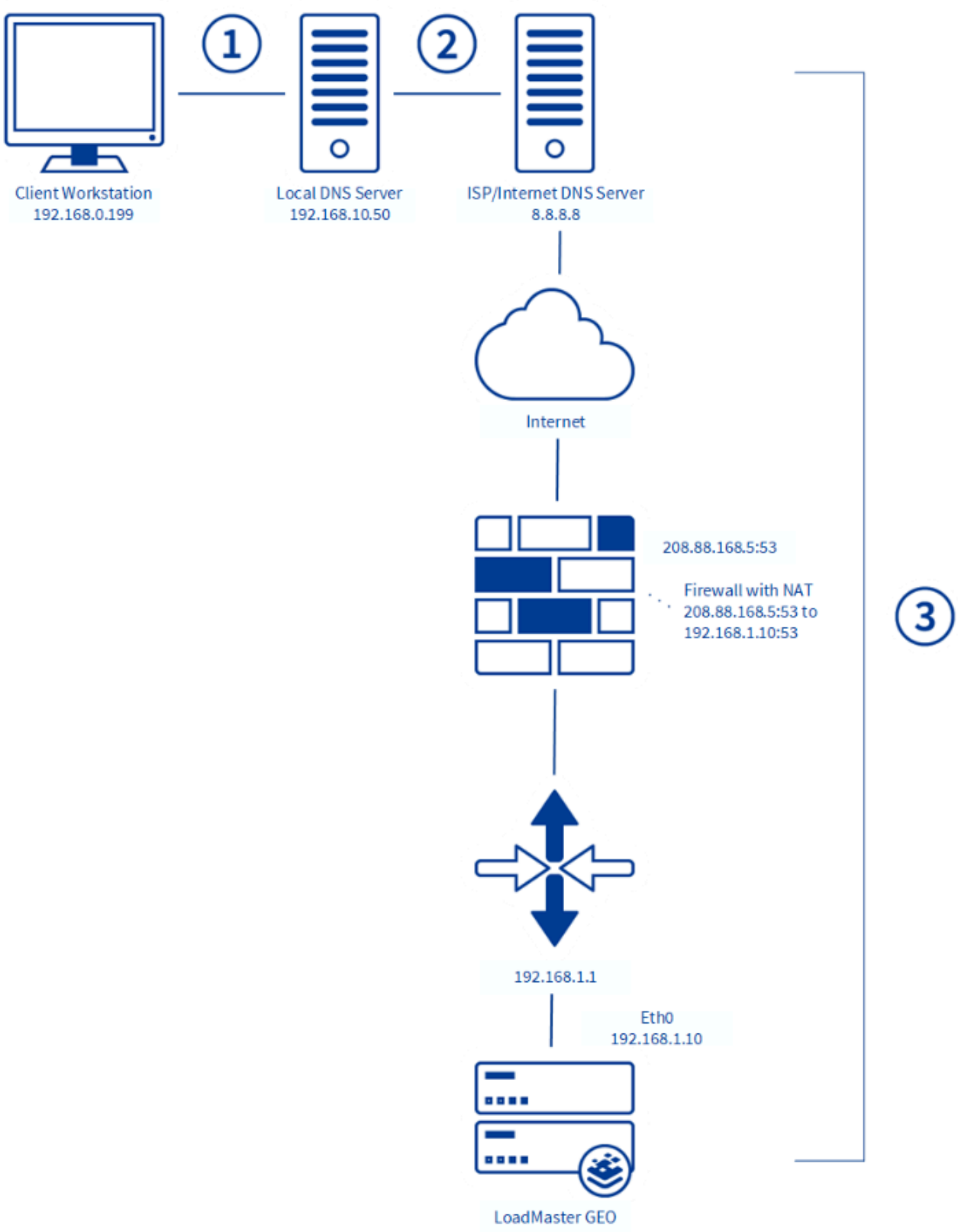
Note: If your LoadMaster version is below 7.2.57, we do not recommend a Layer 3 source IP NAT to the LoadMaster as it will mask source IP visibility during geographical coding operations, all devices before the LoadMaster should be transparent.In 7.2.57, the EDNS Client Subnet (ECS) feature was introduced. For further information, refer to the Global section.

The LoadMaster(s) can be located on the DMZ with no large-scale network changes required. As shown in the diagram above, the default gateway of LoadMaster should point to the firewall.

Client Source IP

Client Source IP

When referring to client source IP, we are taking about the client resolver of the workstation, not the source IP of the workstation or its corresponding NAT to the Internet. This is an important concept to understand; client IPs are of the corresponding DNS resolver. The LoadMaster's geographical encoding operations are based on this client IP. A common deployment for client DNS resolvers is depicted in the diagram below.

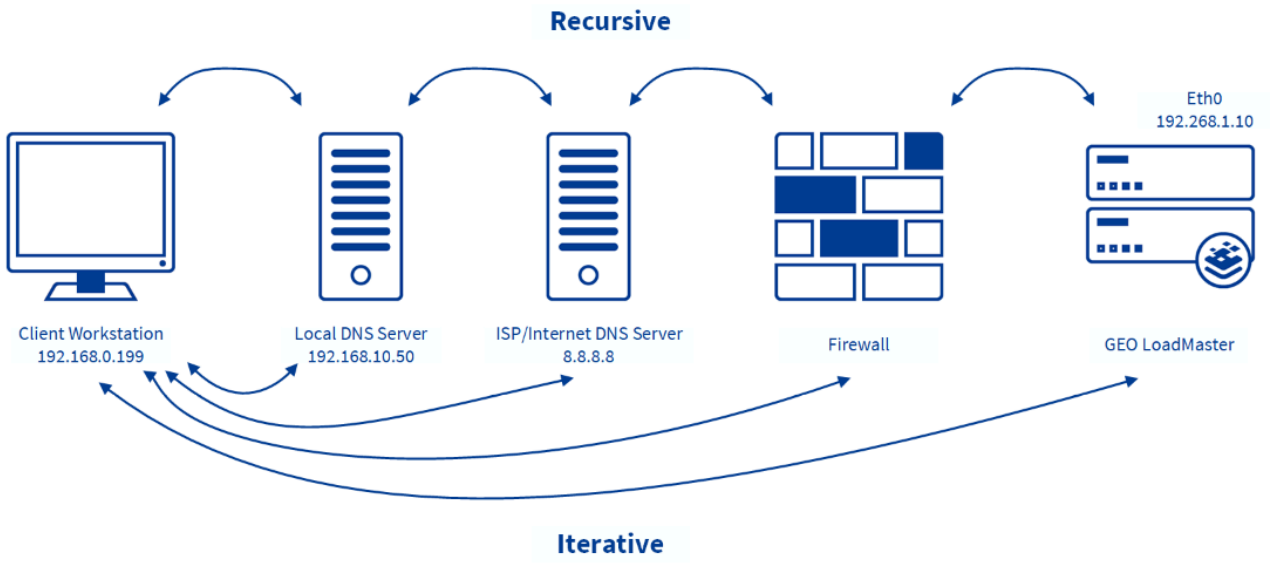


In the illustration above, the following steps occur:

1. The client workstation asks the local DNS server for a translation of www.web.example.com.
2. The local DNS server forwards the request to an ISP or Internet DNS server.
3. The ISP/Internet server has the relevant A records and NS records pointing to the LoadMaster.
4. The GEO LoadMaster responds to the DNS query with an appropriate answer.

It is important to understand that it is step 3, within the described configuration, which defines the client IP address as presented to the LoadMaster, not step 1 or step 2.

If the firewall is transparent, the GEO LoadMaster will see the client as the ISP. If the firewall is NATing the traffic, the GEO will see the client IP address as the firewall.



The above diagram illustrates the difference between recursive and iterative DNS.

With recursive DNS:

1. A public client checks the local DNS server for the IP address of the FQDN.
2. If the Local DNS Server cannot provide the IP address, the local DNS requests the address from the ISP/ internet DNS server.
3. If the ISP/internet DNS server cannot provide the IP address, it requests the address from the firewall.
4. If the firewall cannot provide the IP address, it requests the address from the GEO LoadMaster.
5. The return traffic sends answers back to each device along the chain in the network.

In recursive DNS, the GEO LoadMaster sees the client as the ISP server. Please bare this in mind when using location-based or proximity scheduling.

With iterative DNS:

1. The client checks the local DNS server for the IP address of the FQDN.
2. The local DNS server tells the client to contact the ISP/internet DNS server.
3. The client checks the ISP/internet DNS server for the IP address of the FQDN.
4. The ISP/internet DNS server tells the client to contact the firewall.
5. The client checks the firewall for the IP address of the FQDN.

6. The firewall tells the client to contact the GEO LoadMaster.
7. The client checks the GEO LoadMaster for the IP address of the FQDN.
8. The GEO LoadMaster answers the DNS query.

These are all separate connections.

In LoadMaster firmware version 7.2.57, a checkbox named **EDNS Client Subnet (ECS)** was introduced. ECS is an option in the Extension Mechanisms for DNS that allows a recursive DNS resolver to specify the subnetwork when making a DNS query on behalf of the host or client. For further information, refer to the Global section.

DNS Integration/Delegation

You must create a DNS delegation for the client's DNS request to be forwarded to the LoadMaster. This must be done for both private and public clients. To avoid confusion, this is explained from two perspectives:

- **The application user's point of view:** From the application user's point of view, the FQDN is delegated to the GEO LoadMaster. A user delegates the FQDN **mail.domain.com** to the GEO LoadMaster.
- **The DNS administrator user's point of view:** From the DNS administrator's point of view, the sub-domain is delegated to the GEO LoadMaster. A DNS administrator delegates the subdomain ***mail.domain.com** to the GEO LoadMaster. Any request matching this is forwarded to the GEO LoadMaster. For example:
  - Sales.mail.domain.com
  - QA.mail.domain.com
  - support.mail.domain.com
  - *.mail.domain.com
  - mail.domain.com

All of the FQDNs in the sub-domain **mail.domain.com** are delegated to the GEO LoadMaster including the FQDN **mail.domain.com** itself. In most cases, the only FQDN that matters is **mail.domain.com**. In this scenario, there are no other records in this sub-domain, for example, **Sales.mail.domain.com** and **QA.mail.domain.com**.

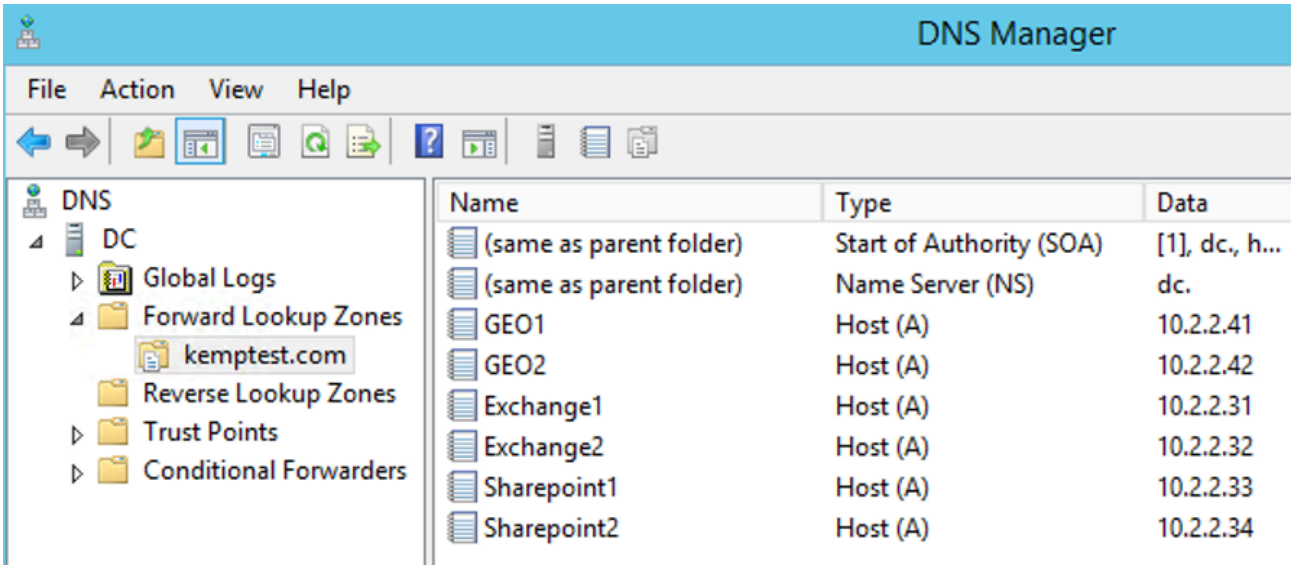
You can integrate the LoadMaster with your authoritative DNS with only a few DNS records:

1. Create a new A record which is pointed to the LoadMaster, for example **lm1.example.com**. Create the corresponding PTR record for the reverse proxy lookup by IP. Forward-confirmed reverse DNS support is required.
2. For each hostname that must be delegated to the LoadMaster, create an NS record and set the value to the A record created for the LoadMaster in the previous step, for example, **www.web.example.com** to **lm1.example.com**.

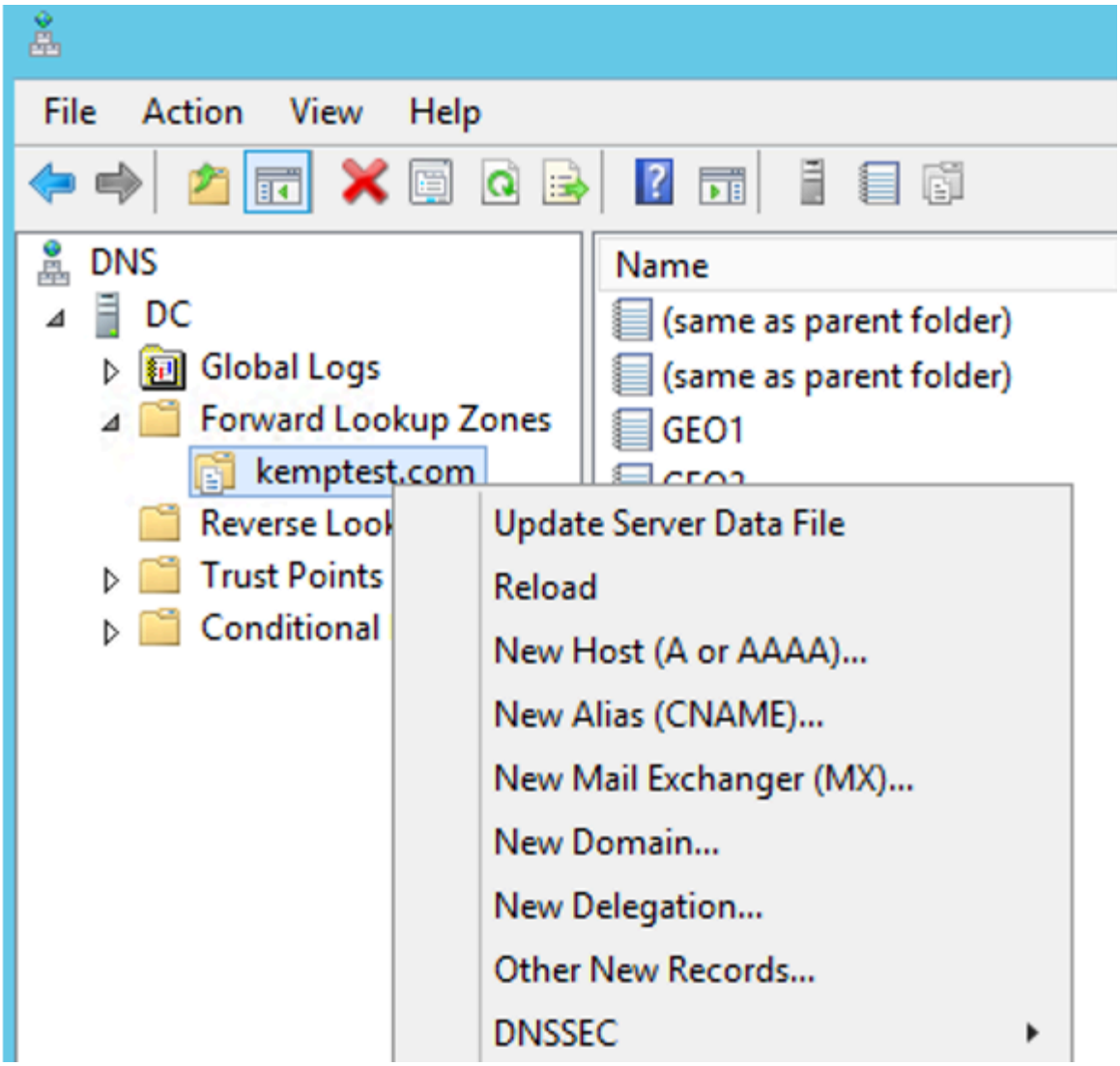
When using GEO LoadMaster active/active configuration, repeat step 1 for the second LoadMaster using a unique hostname, for example **lm2.example.com**. Repeat step 2 using the second LoadMaster. This results in two NS records for **www.example.com**; one pointing to **lm1.example.com** and one to **lm2.example.com**.

Here are some steps with screenshots:

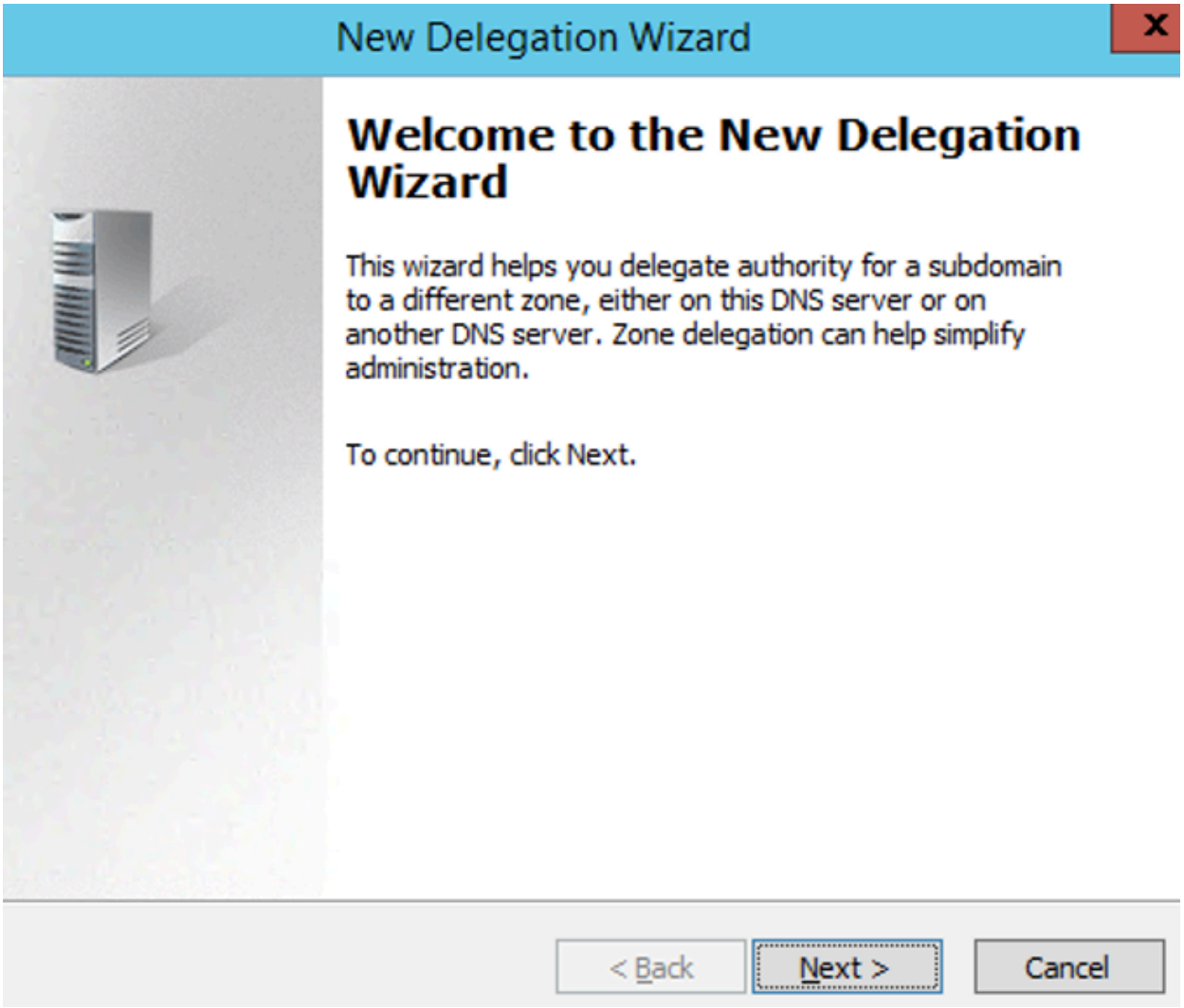
Note: There may be a difference in the following steps depending on the DNS server selected (internal Microsoft DNS server, external, or third party DNS providers) but the purpose of creating the records remains the same.



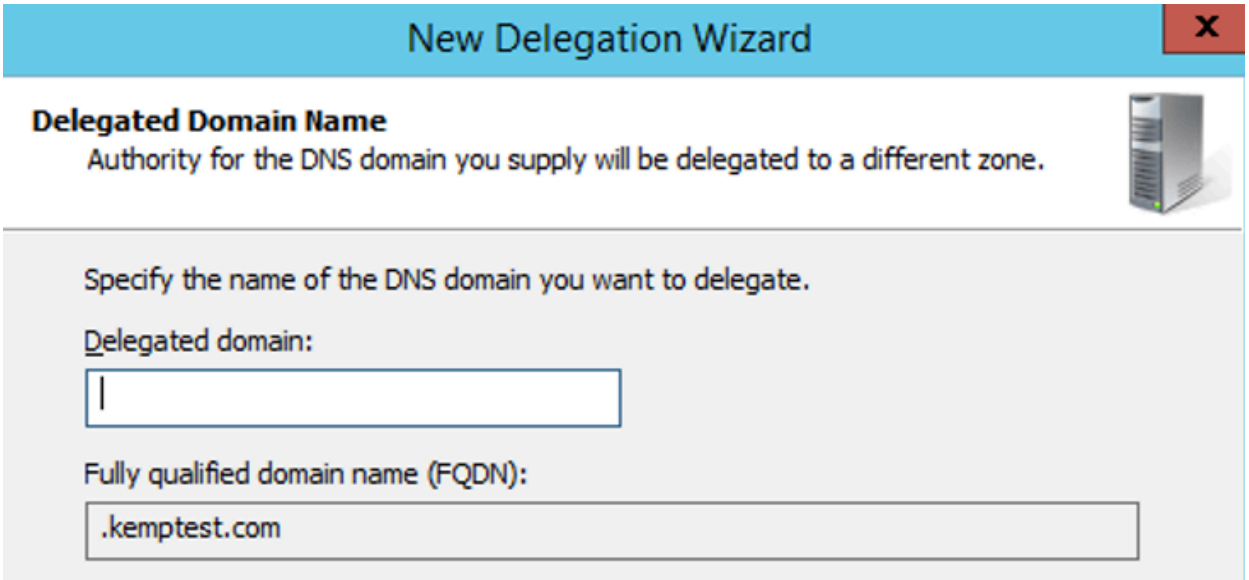
1. Open the DNS Manager. This shows existing records and records already created for GEO LoadMasters.



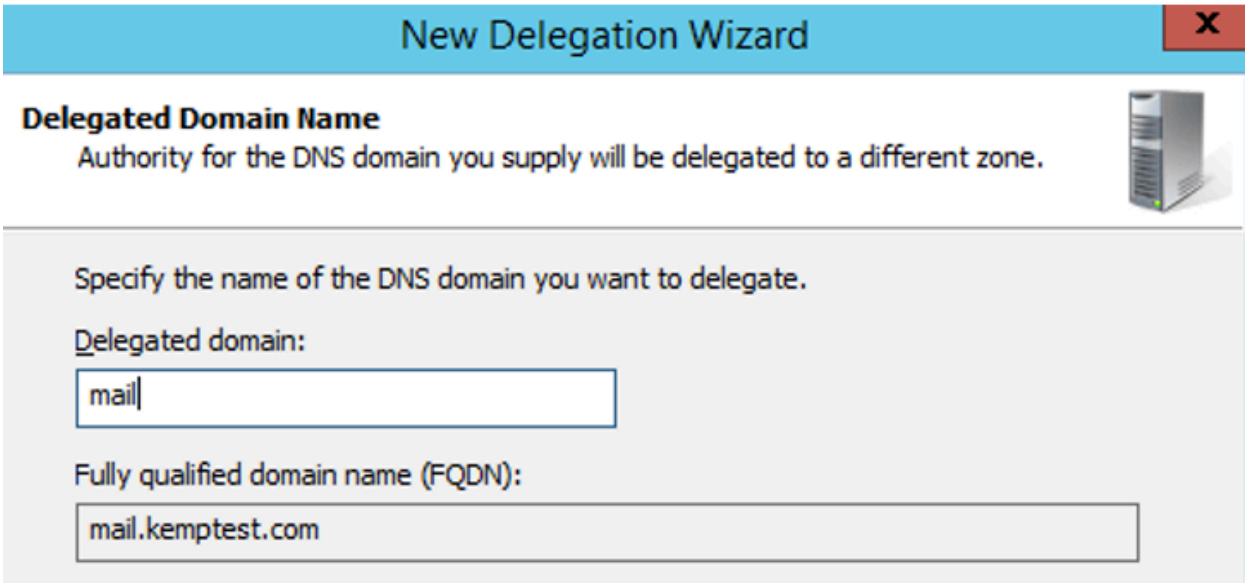
2. Right-click the domain and select **New Delegation**.



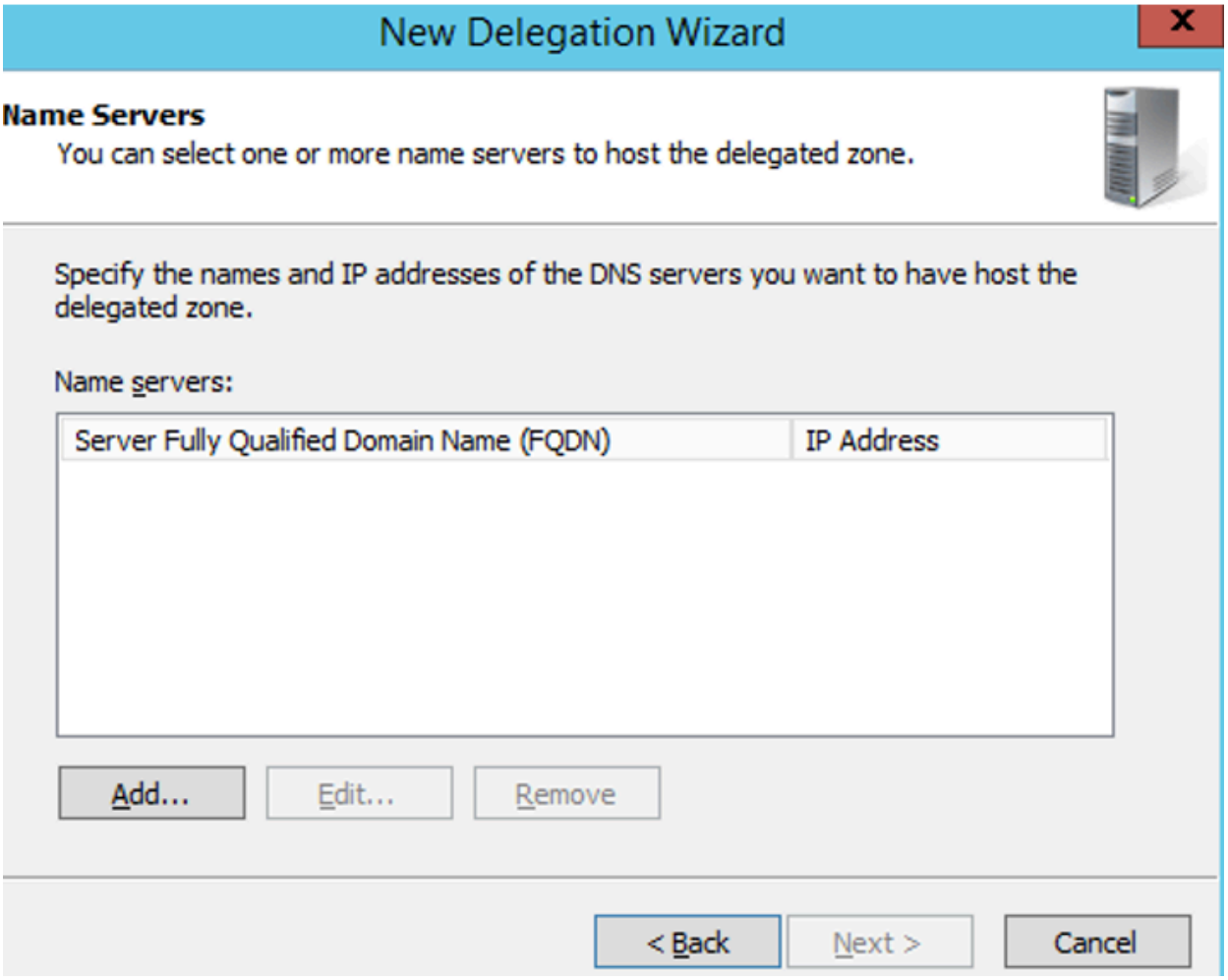
3. Click **Next** on the new delegation wizard.



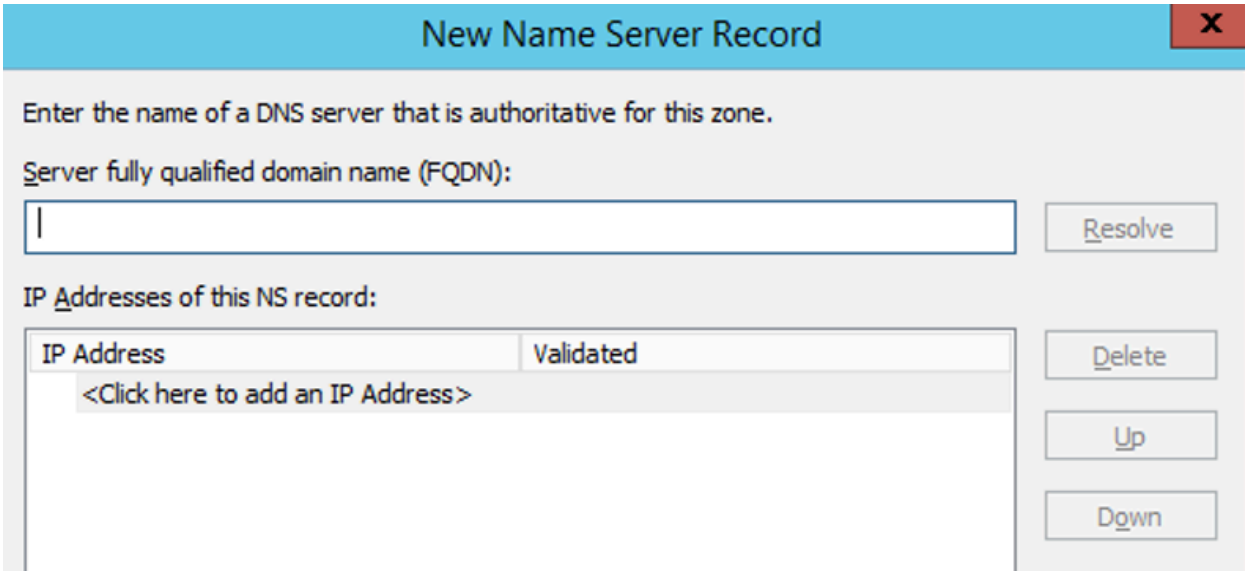
4. Set this to the FQDN/sub-domain that you want to delegate.



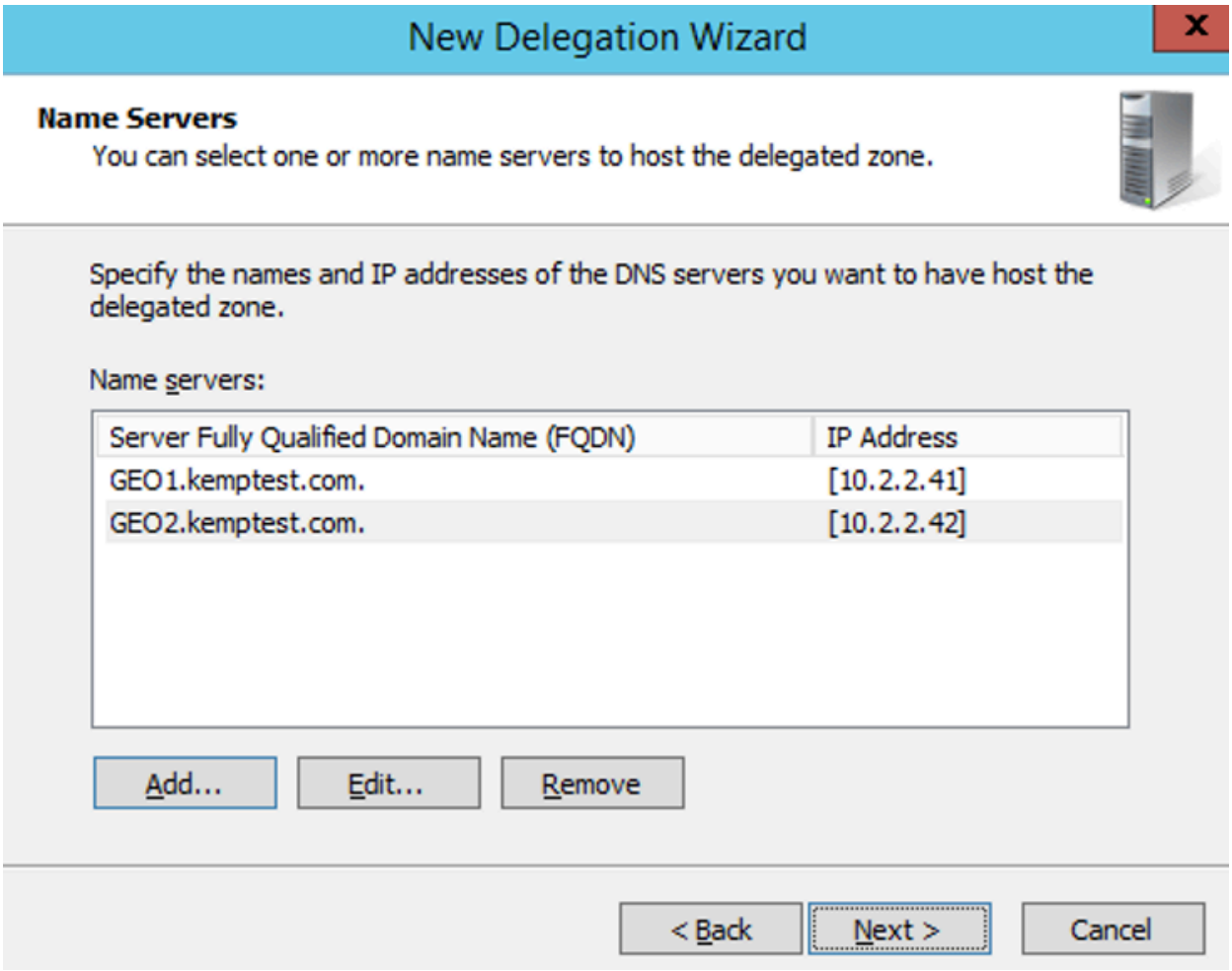
5. In this example, the FQDN mail.kemptest.com (sub-domain *.mail.kemptest.com) is delegated.



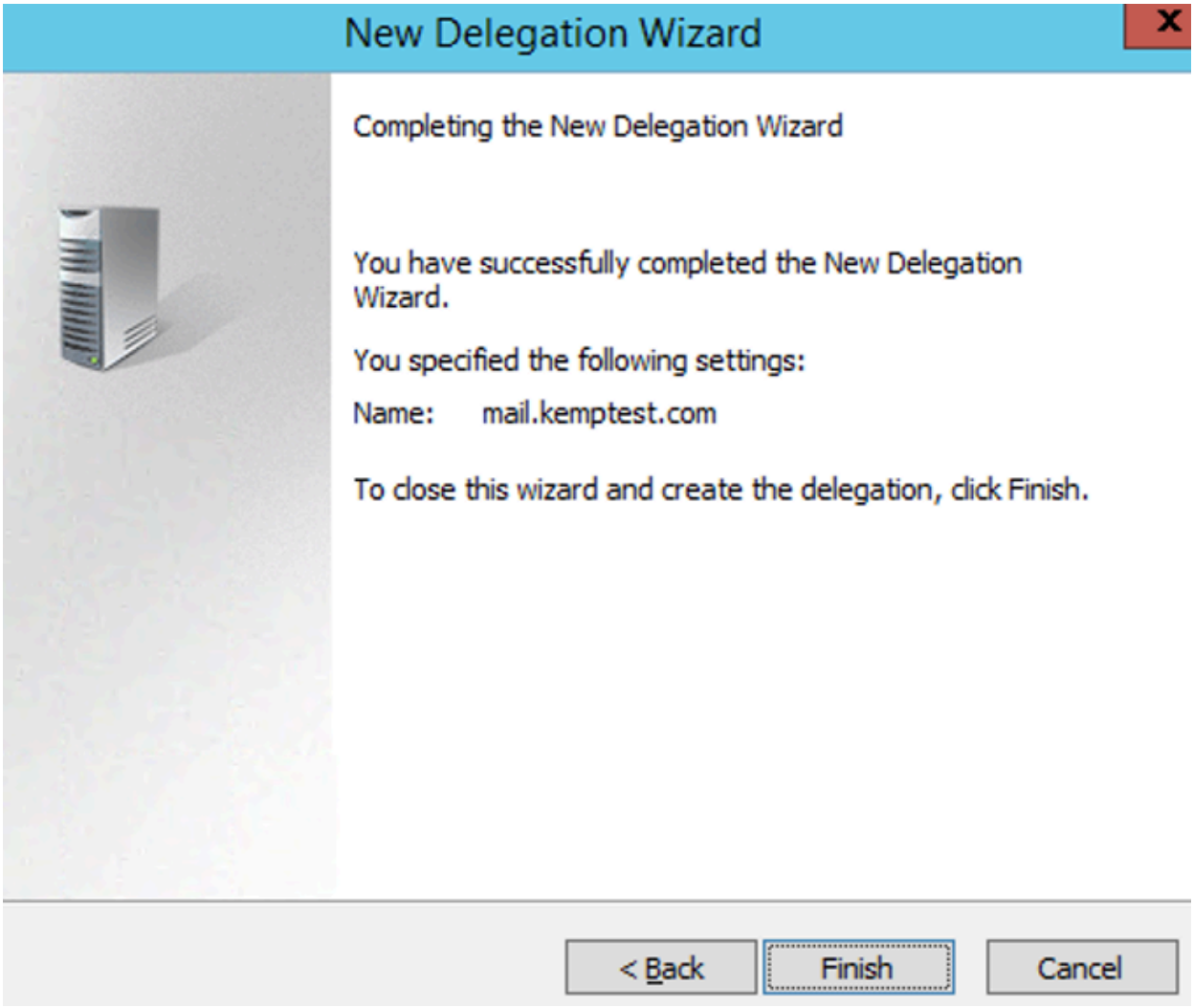
6. Select what to delegate this FQDN/sub-domain to the GEO LoadMaster.



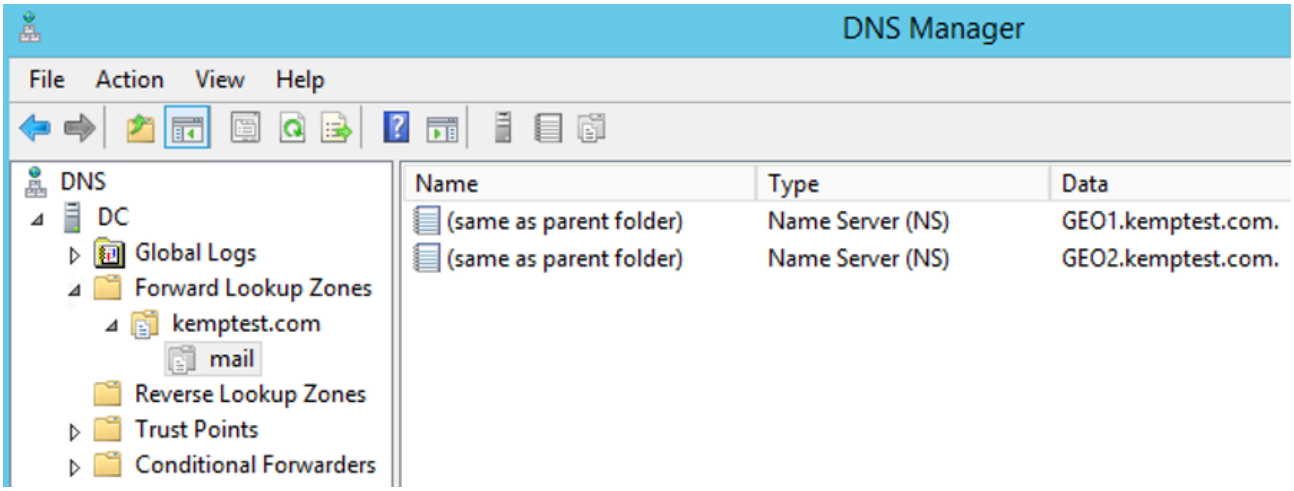
7. Add each GEO LoadMaster individually.



8. Delegate this FQDN/sub-domain to these GEO LoadMasters.



9. Click **Finish**.



Under the domain **kemptest.com** there is now a sub-domain that has a delegation and two NS records pointing to the two GEO LoadMasters.

GEO Miscellaneous Params

Miscellaneous GEO parameters can be configured by going to **Global Balancing > Miscellaneous Params** in the LoadMaster WUI.

Zone



Zone Name

The name of the zone when using DNSSEC. To configure a **Zone Name** appropriately, the DNS server must first be consulted. Once the Zone has been acquired, populate the Zone in this field to indicate the Authoritative Zone. Zone Names are required when configuring DNSSEC.

In relation to DNSSEC, the configured zone defines which FQDNs are signed with DNSSEC.

So, if the following FQDNs are configured:

- one.zone.com
- two.zone.com
- one.other.net
- two.other.net

If the **Zone Name** is set to **zone.com**, then the first two FQDNs are the ones that get signed because they fall under the configured zone, but the others that are outside the zone do not.

Outside of DNSSEC, the main effect of setting a zone would be that if the **Apply to Zone Only** check box is enabled, the configured Source of Authority (SOA)/Name Server (NS) will only be applied to the zone FQDNs, and the others get the default values for those.

If **Apply to Zone Only** is not checked, all FQDNs get the configured SOA values if they have been set.

There may be no need to set a **Zone** unless you are using DNSSEC.

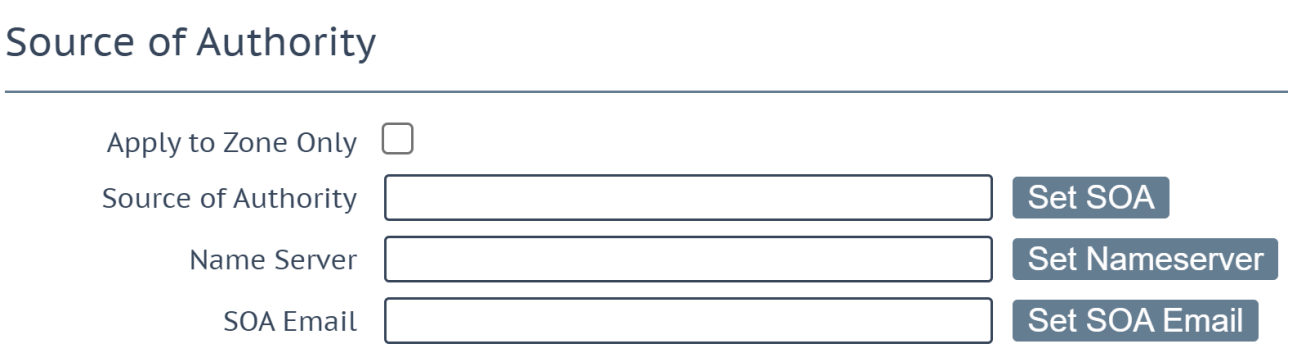
Note: If a **Zone Name** is configured, a **Name Server** must also be configured (otherwise there will be a SERVFAIL).

Note: As of LoadMaster version 7.2.60.1, underscores are supported in this field.

Source of Authority

Configuration of global parameters controls the behavior of the entire LoadMaster. The Source of Authority (otherwise known as Start of Authority) information is not required for basic functionality; however, it is recommended to populate this metadata to accurately represent the LoadMaster DNS server.

Note: In LoadMaster firmware version 7.2.52, the **Zone Name** field moved to the new **Zone** section and a new **Apply to Zone Only** check box was added to the **Source of Authority** section.



Example **Source of Authority** values, and descriptions of each of the fields, are provided below:

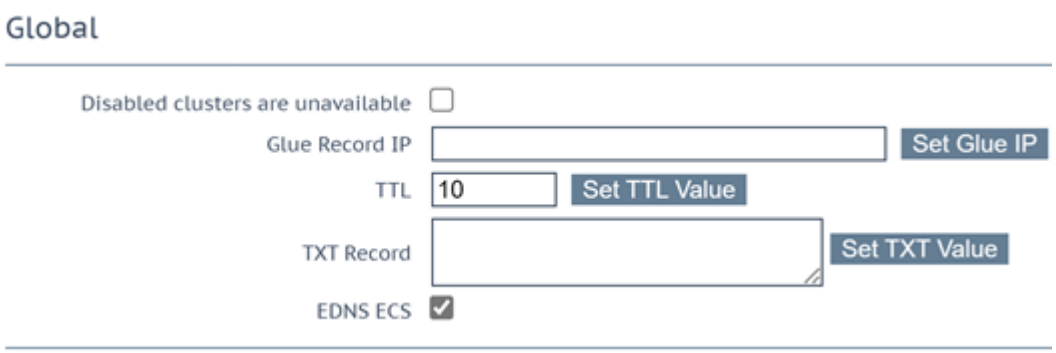
Field	Example	Description
Apply to Zone Only		If this option is enabled, the Source of Authority (SOA) parameters are applied only to the zone. If it is disabled, the SOA parameters apply to all Fully Qualified Domain Names (FQDNs). The **Apply to Zone Only** option is disabled by default.
Source of Authority	kemptechnologies.com	The name of the domain owner. The default value is **ns.<FQDNorZone>**.
Name Server	GEO1.kemptechnologies.com	The name of the DNS server The maximum number of characters permitted in this field is 1022. If a zone is configured, a **Name Server** must also be configured (otherwise there will be a SERVFAIL). The default value is **ns.<FQDNorZone>**.

Field	Example	Description
SOA Email	hostmaster.example.com	Email address of the person responsible for the zone and to which email may be sent to report errors or problems. This is the email address of a suitable DNS administrator but more commonly the technical contact for the domain. By convention (in RFC 2142) it is suggested that the reserved mailbox hostmaster is used for this purpose but any valid email address will work. **Note:** The format is **<MailboxName>.<Domain>.com**, for example, **hostmaster.example.com** (uses a full stop (**.**) rather than the usual **@** symbol because the **@** symbol has other uses in the zone file) but mail is sent to **hostmaster@example.com**. The default value is **hostmaster.<FQDNorZone>**.

The default values for the **Source of Authority**, **Name Server**, and **SOA Email** use the zone for any FQDNs that fall under that zone instead of the FQDN (if one has been set).

Note: As of LoadMaster version 7.2.60.1, underscores are supported in the **Source of Authority**, **Name Server**, and **SOA Email** fields.

Global



Disabled clusters are unavailable

As of LoadMaster firmware version 7.2.53, a new check box named **Disabled clusters are unavailable** has been introduced. This option is disabled by default. When it is enabled, requests to the cluster are dropped if a GEO cluster is disabled. The cluster name on the **Global Balancing > Manage FQDNs** page of the User Interface (UI) will also be displayed in red text.

Glue Record IP

In LoadMaster firmware version 7.2.52, a new text box was introduced called **Glue Record IP** which allows you to set the IP address of the name server to return in additional records in a DNS response. Both IPv4 and IPv6 addresses are supported.

Glue records appear in query results if the following conditions are met:

- A **Zone** has been configured
- At least one **Name Server** has been configured and it belongs to the zone
- The FQDN being queried is part of that **Zone**

For each name server that belongs to the zone, its glue record is returned.

Query failures occur when a glue record is to be returned, but it is not present on the system.

You can currently add glue records to the LoadMaster in the following ways:

- In **Global Balancing > Miscellaneous Params** in the **Glue Record IP** field you can add a single glue record IP address and it will always correspond to the first name server configured in the **Name Server** field. The **Glue Record IP** field defaults to 0.0.0.0 if it is not set. The first Name Server is always guaranteed to have a glue record (0.0.0.0 if not set).
- If more than one name server is configured that require glue records, a workaround is to add the name server (or servers) as an FQDN in **Manage FQDNs** and ensure that it has at least one IP address configured. This FQDN then acts as a glue record from BIND's point of view.

Note: If you change the configuration to a scenario where a SERVFAIL occurs due to the lack of a glue record, the issue may not manifest itself until GEO is restarted because BIND appears to be able to mask the issue by caching previous glue records.

TTL

The Time To Live (TTL) value dictates how long the reply from the GEO LoadMaster can be cached by other DNS servers or client devices. This value should be as practically low as possible. The default value for this field is 10. The time interval is defined in seconds.

TXT Record

In LoadMaster firmware version 7.2.52, support for the TXT (Text) record type was added to the GEO functionality. A TXT (text) record is essentially unformatted data that can be used for almost any purpose, but typically contain information to be consumed by clients to classify a domain in some way, provide details about a domain, or specify resources available within a domain.

The configured record is returned for a TXT request on any Fully Qualified Domain Name (FQDN).

A maximum of 127 characters can be entered as the global TXT record.

The following are not currently supported:

- Multiple strings within the record: Some DNS providers allow you to put multiple strings in one entry using quotes, for example, "string 1" "string 2" "string 3". Progress Kemp does not currently allow this , so you can only have "string 1".
- Non-ASCII characters.

EDNS Client Subnet (ECS)

In LoadMaster firmware version 7.2.57, a checkbox named **EDNS Client Subnet (ECS)** was introduced. ECS is an option in the Extension Mechanisms for DNS that allows a recursive DNS resolver to specify the subnetwork when making a DNS query on behalf of the host or client.

By default, the **EDNS Client Subnet (ECS)** checkbox is enabled on new installations but if you are upgrading a LoadMaster that previously used GEO functionality then the option is disabled. When enabled, the ECS field (if included in the request) is used to determine the client location. When disabled, this field is ignored.

Note: It is possible that a client that has EDNS enabled may be sending requests through recursive DNS servers that are not enabled for EDNS. That means the client subnet will be dropped from the UDP packet that is received by the LoadMaster. If the EDNS client subnet information is removed it will not be available for the LoadMaster to act on.

Resource Check Parameters

Resource Check Parameters define the GEO health checking that occurs from LoadMaster to GEO Clusters and Real Servers. For more information on clusters, refer to the Scheduling Methods section. The default values for the **Resource Check Parameters** are as follows:

- **Check Interval**: 120
- **Connection Timeout**: 20
- **Retry attempts**: 2

Depending on the behavior, the wait can take up to (<Retries>+1)*<Timeout>:

- If there is no response at all, it waits the maximum duration as stated above
- If the service returns a rejection of some form, it may take significantly less time to fail

Stickiness



Global Server Load Balancing (GSLB) Persistence, also known as ‘Stickiness’, is the property that enables all name resolution requests from an individual client to be sent to the same set of resources until a specified period of time has elapsed. This ensures that users are able to retrieve and interact with session-specific

data. **Stickiness** can be set globally in the **Miscellaneous Params** section, or for an individual FQDN.

If connecting from a client to the GEO LoadMaster directly, the GEO LoadMaster keeps a persistence entry for the request. If connecting from a DNS server to the GEO LoadMaster directly, the GEO will keep a persistence entry for the request, as will the DNS server. When troubleshooting, ensure to set **Stickiness** to **0** and clear the DNS cache on the DNS server (**Dnscmd /clearcache** on Windows Server).

If EDNS Client Subnet (ECS) option (in **Global Balancing > Miscellaneous Params**) is enabled, the GEO LoadMaster uses the ECS value instead (if one is received) for direct connection to the client or DNS server. If disabled, the GEO LoadMaster uses the client or DNS server request's source IP address for direct connection.

Note: It is possible that a client that has EDNS enabled may be sending requests through recursive DNS servers that are not enabled for EDNS. That means the client subnet will be dropped from the UDP packet that is received by the LoadMaster. If the EDNS client subnet information is removed it will not be available for the LoadMaster to act on.

For further information, refer to the GEO Sticky DNS, Feature Description.

Location Data Update

You can update the GEO location database with the latest data by doing the following:

1. Go to the Other Downloads page to download the latest GEO database ZIP archive to your local system (for example, your laptop).
2. After download, extract the ZIP archive using the appropriate utility on your local system. The archive contains several files. The file without any extension contains the database update; the other files can be used to check the correctness of the downloaded update file.
3. Open the LoadMaster Web User Interface (WUI) and go to **Global Balancing > Miscellaneous Params**.
4. Click **Choose File** and use the pop-up controls to select the GEO data file from the extracted ZIP file contents on your laptop. Look for the file that does not have a file extension, as in this example: **geodata.patch_2007_03_01_0104**.
5. After the GEO data file has been uploaded and verified by the LoadMaster, click the **Install Update** button to add it to the running system.

Note: The legacy MaxMind GeoLite database is only supported on LoadMaster version 7.2.44 and below. The new MaxMind GeoLite2 database is only supported on LoadMaster version 7.2.45 and above.

GEO System Info / Debug

To access GEO debugging information and options, go to **Global Balancing > Geo System Info / Debug**.



GEO Information

This section provides information about the state of the GEO system, including:

- Config: Displays the last updated date (in format YYYY-MM-DD) and time, version, and total number of FQDNs and IP addresses
- Services: Displays the nameserver, healthcheck, persistence, and GEO process monitor details
- Remote machines: Displays details about configured GEO partners and remote GEO clients
- GEO file system: Displays details about the GEO file system including the number of forward zones, number of reverse zones, and number of DNS views details
- GEO IP Database: Displays the MaxMind database version

If you click the **Refresh** button, the data displayed in the **GEO Information** section gets refreshed.

GEO Debug Options

Restart GEO Services

Clicking **Restart GEO Services** restarts the nameserver, health check, and stickiness services.

GEO Process Monitor

When the **GEO Process Monitor** is enabled, three primary services (nameserver, healthchecks, and persistence) are monitored. If one or more of these services shut down, the LoadMaster attempts to restart them. By default, the **GEO Process Monitor** option is enabled.

The **GEO Process Monitor** setting is synced across High Availability (HA) units. The GEO Process Monitor setting is not synced across GEO partner units.

Automatic Partner Syncing

Enable or disable automatic synchronization of configuration data from this unit to all partners. Disabling the **Automatic Partner Syncing** option may be useful when debugging complex environments. The manual sync button on the page still functions when the automatic sync is disabled.

Sync Partners - Debug Mode

Clicking **Debug Sync** pushes the GEO configuration to the configured partners and logs the connection debug information in the message log.

Retrieve All Remote Cluster VS' - Debug Mode

Clicking **Debug Retrieve** gets the remote Virtual Service data from all configured LoadMaster clusters and logs the connection debug information in the message log.

Enable SSHD debug logs

Clicking **Enable SSHD debug logs** enables SSHD debug logs to debug the incoming connections from remote machines.

Enable GEO Query Logging

Enable bind debug trace logs for GEO.

Note: GEO Query Logging should only be enabled when troubleshooting because it will impact the performance of the LoadMaster.

Open warning log

Open the warning log in a new window. The warning logs also contain any SSHD debug logs if they are enabled on this page.

Open nameserver log

Open the name server log in a new window.

Fully Qualified Domain Name (FQDN)

A Fully Qualified Domain Name (FQDN) is the hostname in which you need to perform load balancing. The FQDN can be any hostname in the top-level domain or a hostname that is nested as a sub-domain. Each FQDN can be an A (IPv4) or AAAA (IPv6) record.

Guidance on the number of public IP addresses you need to have available for publicly delegating FQDNs for GEO is below:

- One public IP address is needed for each LoadMaster/HA pair that is configured.
- One public IP address is needed for each endpoint being contacted.

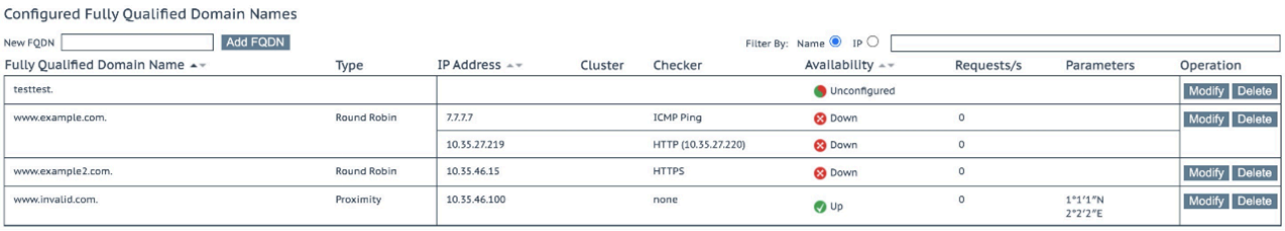
Each public IP must be tied to an endpoint, or if the end point has a private IP address then the public IP address must NAT to it.

Each distinct hostname must be configured in the LoadMaster individually.

You can create an FQDN for www.example.com and also www.kemptechnologies.com.

FQDN Filtering and Sorting

You can filter the FQDNs based on FQDN Name or IP Address using the filter text box.



Filter By Name

By default, radio button for FQDN Name is selected and when you enter any FDQN Name in the search text box, it displays the results for related FQDN entries.

Filter By IP

If you select the radio button for FQDN IP and enter any FQDN IP in the search text box, it displays the results for FQDN entries which have a related IP address.

If you enter any text in the filter text box that is contained in the name/IP, the list will be instantly filtered to show the matching results. If you enter some text in the filter text box that is not in any name/IP (depending on the radio button selected) the text box flashes red and the text that does not match is deleted.

In the FQDN table, you can sort the FQDN entries available for FQDN Name, IP Address, and Availability options using up/down arrow on FQDN table header.

- For FQDN Name, entries can be sorted in alphabetical order or reverse alphabetical order.
- For IP Address, entries can be sorted first by IP version (IPv4 followed by IPv6), then by IP address or

reverse alphabetical order.

- For Availability, entries are sorted by the Down status first, followed by the remaining FQDNs only when there are Up and Down status FQDNs available the list. If there are multiple FQDNs present in the list with multiple statuses like Up, Down, Disabled, and Unconfigured then sorting occurs in the following order:
  - Unconfigured
  - Disabled
  - Down
  - Up

  In reverse order:
  - Up
  - Down
  - Disabled
  - Unconfigured

Add an FQDN

To add an FQDN, follow the steps below:

1. In the main menu, select **Global Balancing** and **Manage FQDNs**.
2. Click the **Add FQDN** button.



3. Enter an FQDN name, for example **www.example.com** in the **New FQDN** textbox.

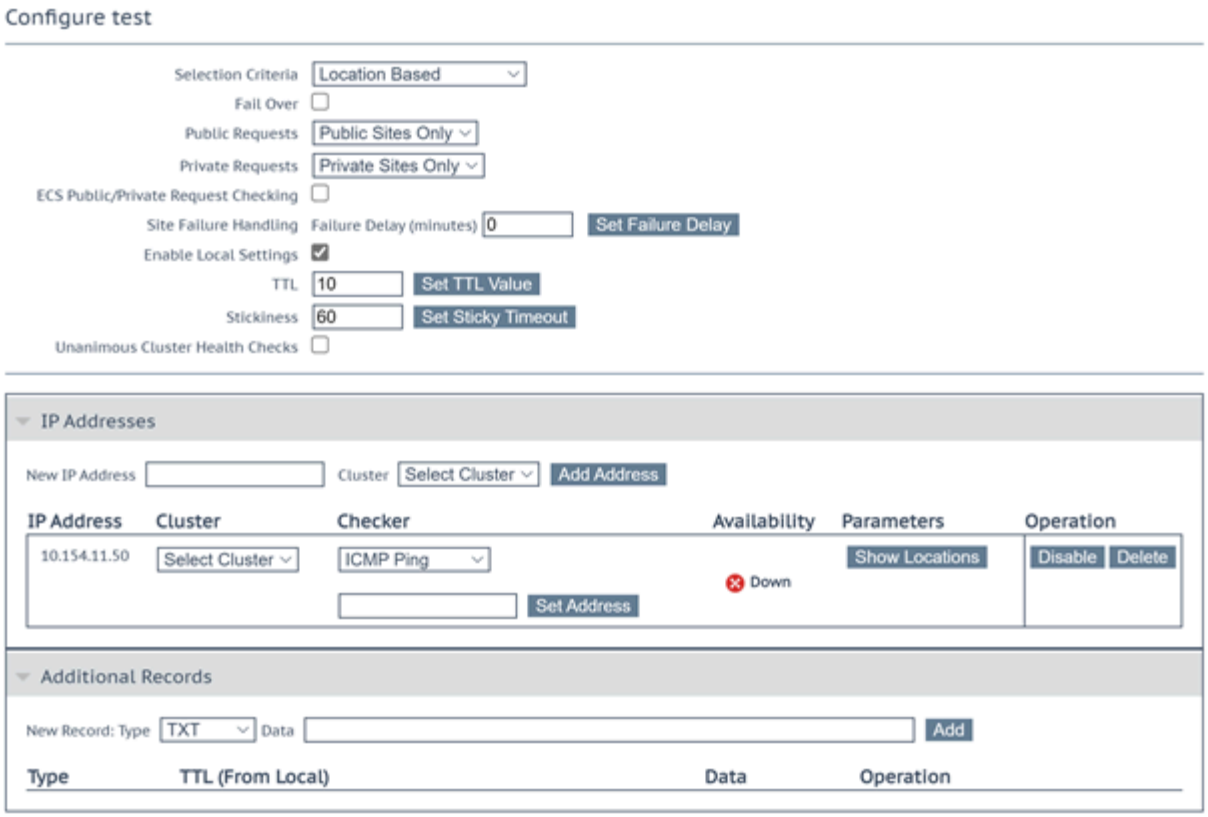
   Note: As of LoadMaster version 7.2.60.1, underscores are supported in this field.

   Note: In LoadMaster firmware version 7.2.54.1 and earlier, the maximum number of possible FQDNs allowed is 256. For LoadMaster firmware version 7.2.55 or above, the number of possible FQDNs is limited by the size of the RAM available.

   Note: The FQDN can be a maximum of 63 characters long. Otherwise, a pop-up message appears that says "FQDN must be 63 characters or less".

   Note: Wildcards are supported here, for example ***.example.com** matches anything with **.example.com** ending.

4. Click the **Add FQDN** button.
5. Click **OK** on the message that appears.



6. Select the relevant load balancing algorithm from the **Selection Criteria** drop-down list.
7. If the **Selection Criteria** is set to **Location Based**, you can specify whether or not to allow **Fail Over**.

   Select the relevant options for the **Public Requests** and **Private Requests** drop-down lists.

Note: When the **Fail Over** option is enabled, if a request comes from a specific region and the target is down, the connection will fail over and be answered with the next level in the hierarchy. For example, if the **Selection Criteria** is **Location Based -** the country comes first in the hierarchy, then continent. If this is not available, the connection is answered by the nearest (by proximity) target. If this is not possible, the target with the lowest requests is picked. The **Fail Over** setting affects all targets.

---

8. The **Isolate Public/Private Sites** setting has been enhanced as of version 7.1-30. The checkbox has been migrated to two separate dropdown menus to allow more granular control of DNS responses. Existing behavior has been preserved and is migrated from your current setting, ensuring that no change in DNS responses is experienced. These new settings allow administrators finer control of DNS responses to configured FQDNs. Administrators may selectively respond with public or private sites based on whether the client is from a public or private IP. For example, administrators may wish to allow only private clients to be sent to private sites.

Setting	Value	Client Type	Site Types Allowed
Public Requests	Public Only	Public	Public
	Prefer Public	Public	Public, Private if no public

Setting	Value	Client Type	Site Types Allowed
	Prefer Private	Public	Private, Public if no private
	All Sites	Public	Private and Public
Private Requests	Private Only	Private	Private
	Prefer Private	Private	Private, Public if no private
	Prefer Public	Private	Public, Private if no public
	All Sites	Private	Private and Public

The following table outlines settings and their configurable values:

9. Enable/disable the **ECS Public/Private Request Checking** check box, as needed. When disabled, the device uses the client request's source IP address to determine if the request is public or private. When enabled, the device uses the EDNS Client Subnet (ECS) value instead (if one is received) to determine if the request is public or private. This option becomes inactive in either of the following conditions:

   - The **EDNS Client Subnet (ECS)** option (in **Global Balancing > Miscellaneous Params**) is disabled.
   - The **Public Requests** and **Private Requests** values are both set to **All Sites**.

   The **ECS Public/Private Request Checking** was added to the modify FQDN screen in LoadMaster firmware version 7.2.58.

   The following table summarizes the behavior depending on the configuration:

EDNS Client Subnet (ECS) setting under Miscellaneous Params	Public/Private settings	ECS Public/Private Request Checking - Disabled	ECS Public/Private Request Checking - Enabled
Disabled / Off	Any	Public/private check is based on the source IP address	Public/private check is based on the source IP address as ECS for GEO is disabled
Enabled / On	If either option (**Public Requests** or **Private Requests**) is not set to **All Sites**	Public/private check is based on the source IP address	Public/private check is based on the ECS IP address
Enabled / On	If both **Public Requests** and **Private Requests** are set to **All Sites**	Public/private check is based on the ECS IP address - option is greyed out	Public/private check is based on the ECS IP address - option is greyed out

10. A **Failure Delay (minutes)** can be set if needed. If a **Failure Delay** is set, another option called **Site**

Recovery Mode becomes available. Refer to the Enabling Fail Over section for further information on these options.

Note: Following a completely failed health check, the GEO LoadMaster waits for the specified number of minutes before taking the site out of rotation.

11. Enable/disable the **Enable Local Settings** check box, as needed. If enabled, configure the **TTL** and **Stickiness** options.
12. Enable or disable **Unanimous Cluster Health Checks**. If this option is enabled, if any IP addresses fail health checking – the other FQDN IP addresses in the same cluster is forced down. For further information, please refer to the Scheduling Methods section.
13. Enter the IP address of the domain in the **IP address** text box.

Note: We do not recommend downgrading the LoadMaster firmware version to a previous version where the endpoint limit of IP addresses per FQDN is smaller than the number of IP addresses in your configured FQDNs.

Note: The entry limit was increased to 256 IP addresses in LoadMaster firmware version 7.2.57. If you attempt to add more than this, you get an error message saying **Limit of 256 IP Addresses has been reached for the FQDN**. It is recommended that the LoadMaster should have sufficient memory space (minimum 8GB of RAM) to configure the maximum of 256 IP addresses per FQDN.

Note: In LoadMaster firmware versions prior to 7.2.57, there is an entry limit of 64 IP addresses per FQDN.

14. If needed, select the **Cluster** name.
15. Click **Add Address**.
16. Select the type of health checking to be performed from the **Checker** drop-down list. For further information regarding health checking options, refer to the FQDN Health Check Options section.
17. Select the **Additional Records** type to configure records for a specific FQDN. You can add, modify, or delete additional TXT, CNAME, and MX records to an FQDN. For more information and instructions, refer to the Additional Records section.

Note: Underscores are supported in the **Data** field for each of the record types.

FQDN Health Check Options

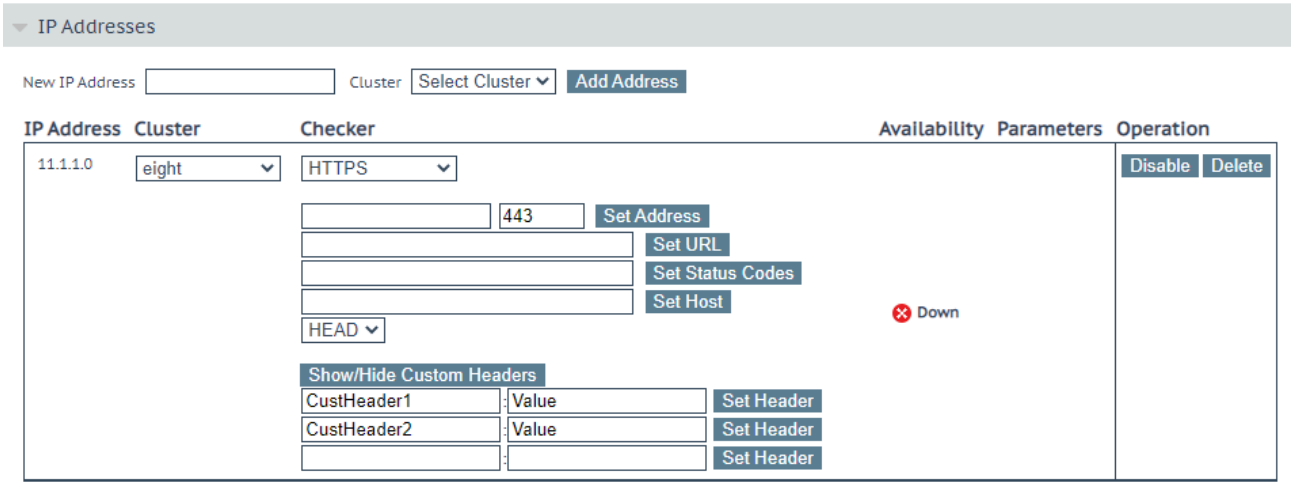
The **Checker** options in the **Configure FQDN** screen defines the type of health checking that is performed. The options include:

- **None:** This implies that no health check is performed to check the health status of the machine (IP address) associated to the current FQDN.
- **ICMP Ping:** This tests the health status by pinging the IP address.
- **TCP Connect:** This will test the health by trying to connect to the IP address on a specified port.
- **Cluster Checks:** When this is selected, the health status check is performed using the method associated with the selected cluster.

Note: If there are no clusters configured, the **Cluster Checks** value is grayed out.

- **HTTP/HTTPS:** In LoadMaster firmware version 7.2.53, support was added to perform Layer7 (L7) HTTP and HTTPS health checks on back-end servers within GEO "sites" that are not handled from the LoadMaster for application delivery. In other words, site health determination can be enhanced directly from GEO by checking the health of back-end servers that are not being health-checked by LoadMaster.

Note: HTTP/1.1 is supported (HTTP/1.0 is not supported).



The available options that appear when **HTTP** or **HTTPS** is selected as the **Checker** are as follows:

- **Address:** Set the address and port to use to health check the IP address. The default port is **80** when **HTTP** is selected and **443** when **HTTPS** is selected.
- **URL:** By default, the health checker tries to access the URL forward slash (/) to determine if the machine is available. You can specify a different URL here.
  - The URL must begin with a forward slash (/).
  - The URL cannot contain **http:** or **https:**.
  - The URL can be a maximum of 127 characters.
  - If the URL is left blank, a forward slash (/) is sent by default.
- **Status Codes:** A space-separated list of HTTP and HTTPS status codes that should be treated as successful when received from the server.

  Health check status codes can be set to override default functionality. Without any **Status Codes** set, the following HTTP status codes are considered to be Up:

  - 200-299: Success (for example 200 OK, 202 Accepted)
  - 301: Moved Permanently
  - 302: Found
  - 401: Unauthorized

Additionally, 2xx status codes are subject to pattern matching the response data, if this is configured. Other codes are considered up without pattern matching, even if it is set.

If custom health check codes are set:

- Check codes may be set to a list of numbers, each from 300-599
- Check codes may be up to 127 characters long, which means 32 valid codes
- Any code in the list is considered to have a health check status of Up
- Configured codes override the default set
  - 2xx codes are always considered up in all cases and are subject to pattern matching, if configured
  - Check codes may be official HTTP status codes, unofficial codes or custom-defined user codes – as long as they fall in the range of 300-599
    - For a list of official HTTP status codes, refer to: https://en.wikipedia.org/wiki/List_of_HTTP_status_codes
    - For a list of unofficial codes, refer to: https://en.wikipedia.org/wiki/List_of_HTTP_status_codes#Unofficial_codes
  - Microsoft sub-codes using decimals can be supported, but only by the top-level status code
    - For a list of Microsoft sub-codes using decimals, refer to: https://support.microsoft.com/en-us/kb/943891
    - Sub-codes may not be configured in the Status Codes field – please use the three digit code
    - Sub-codes are grouped by the top-level code

- **Host:** A hostname can be supplied in the request to the server. If this is not set, the server address is sent as the host.
  - There is a limit of 127 characters.
  - Allowed characters: alphanumerics and **-._:**
- **Method:** When accessing the health check URL, the system can use the **GET**, the **POST**, or the **HEAD** method. If **POST** is selected, another field appears to set the POST data. Up to 2047 characters of POST data can be passed to the server.
- **Show/Hide Custom Headers:** When you click the **Show/Hide Custom Headers** option, it displays the custom headers that are to be part of the health check request.
- **Header:** Add a custom header to be part of the health check request.
  - There is a limit of 255 characters for the total check headers string. The first text box allows you to specify a key for the custom header. The second text box allows you to specify a value for the custom header. The value has a maximum length of 128 characters.
  - Allowed characters for header keys: alphanumerics and **_-**
  - Allowed characters for header values: alphanumerics and **_-.+=;()**

Note: You can specify a maximum of four custom headers.

The status of the health check displays in the **Availability** column.

Note: It is not possible to override the GEO health checks on a per-FQDN basis (like you can with Virtual Services).

Note: The **Check Parameters** in **Rules & Checking > Check Parameters** do not apply to GEO. Only the settings in **Global Balancing > Miscellaneous Params** apply to GEO.

Scheduling Methods

The GEO LoadMaster load balances DNS requests – it does not load balance traffic. GEO offers many load balancing algorithms including **round robin**, **weighted round robin**, **fixed weighting**, **real server load**, **location based**, **proximity** , and **all available**.

The selection criterion chosen determines how GEO distributes the incoming requests across the IP address end-points for the FQDN.

The selection criterion can be altered in real-time; previously configured information is retained during a change. Only a single selection criterion is permitted per FQDN and each FQDN can have a unique selection criterion. The following sections outline the selection criteria that are available on the LoadMaster.

Each of these scheduling methods are described below.

Round Robin

With the Round Robin method, incoming requests are distributed sequentially across the IP address end-points.

Note: IP address end-points for an FQDN could be Real Servers, LoadMasters or even Data Centers depending on how the FQDN is configured.

If this method is selected, all the IP address end-points assigned to an FQDN should have similar resource capacity and host identical applications. Subject to this precondition, the round robin system is a simple and effective method of distribution.

However, if the IP address end-points have different capacities, the use of the round robin system can mean that a less powerful IP address end-points receives the next inquiry even though it has not yet been able to process the current one. This could cause a weaker IP address end-points to become overloaded.

This selection criterion is not dependent on the geographical IP database.

Round Robin load balancing can be used for all active data centers, which includes support for weights and a chained failover option for disaster recovery. Round robin scheduling in GEO LoadMasters works the same way as the normal LoadMaster with one exception; when using nslookup, by default it will check for both IPv4 (A) records and IPv6 (AAAA) records which actually sends out two requests.

For example, if you have two sites:

- Request 1 IPv4 A record hits Site 1,
- Request 2 IPv6 record AAAA hits Site 2,
- Request 3 IPv4 A record hits Site 1,

- Request 4 IPv6 AAAA record hits Site 2

When testing:

- Clients looking for IPv4 will always connect to Site 1.
- Clients looking for IPv6 will always connect to Site 2.

To help prevent this during testing – add an odd number of sites.

Weighted Round Robin

This method balances out the weakness of the simple round robin: incoming requests are distributed across the cluster in a sequential manner, while taking account of a static “weighting” that can be pre-assigned per server.

The administrator simply defines the capacities of the servers available by weighting the servers. The most efficient server, **A** for example, is given the weighting 100, whilst a much less powerful server (**B**) is weighted at 50. This means that Server **A** would always receive two consecutive requests before Server **B** receives its first one, and so on.

This selection criterion is not dependent on the geographical IP database.

Fixed Weighted

Fixed weighted scheduling is usually used in Disaster Recovery (DR) sites. The highest weight Real Server is only used when other Real Server(s) are given lower weight values. However, if the highest weighted server fails, the Real Server with the next highest priority number is available to serve clients. The weight for each Real Server should be assigned based on the priority among the remaining Real Servers. When the failed Real Server becomes available, it automatically starts receiving requests.

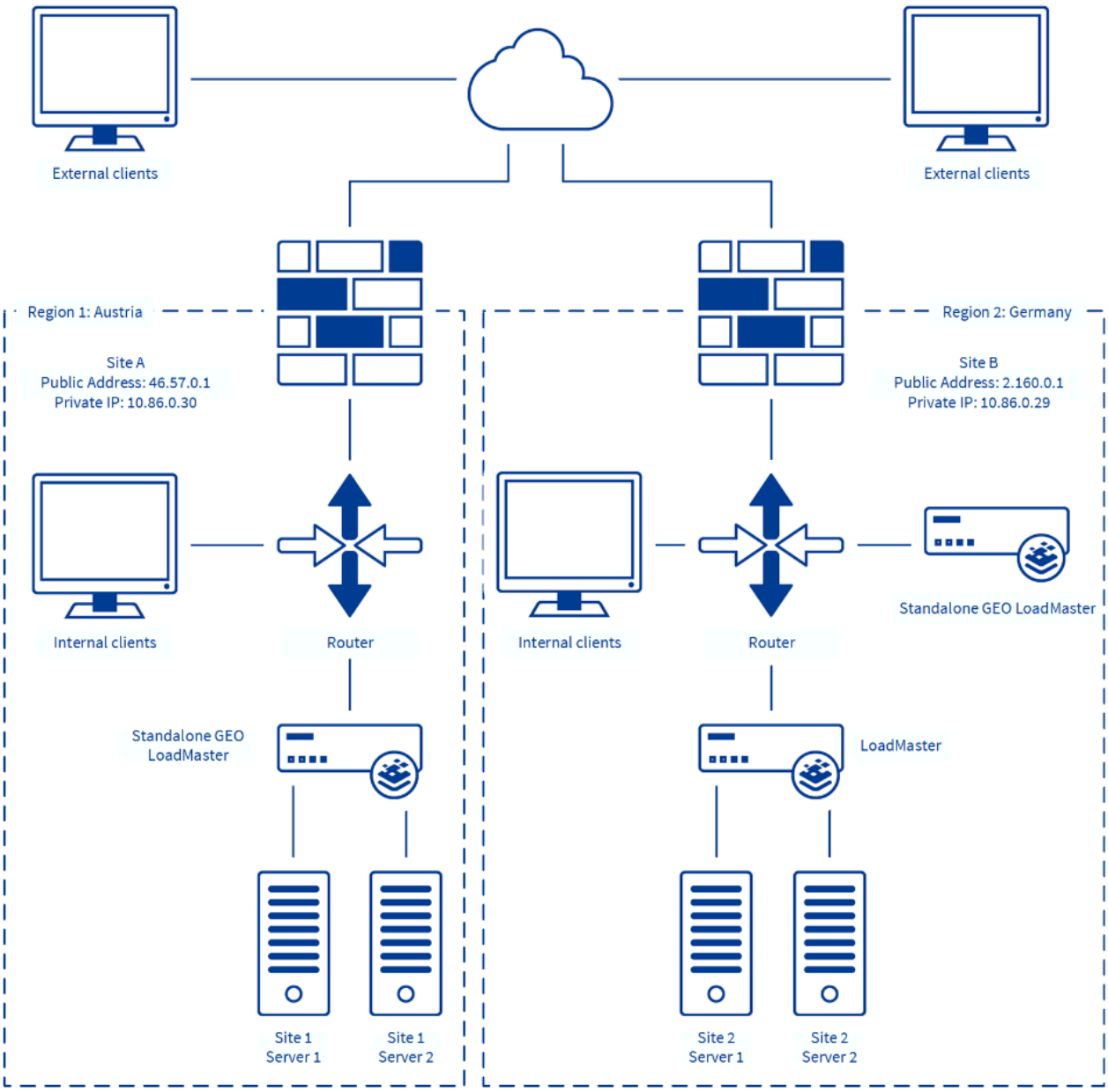
This selection criterion is not dependent on the geographical IP database.

Real Server Load

GEO securely and seamlessly integrates with core LoadMaster functionality to offer Real Server Load balancing, for which GEO uses local data center metrics (provided by the LoadMaster) allowing clients to connect to the most available target. Each IP address end-point in the FQDN must have a **Cluster** assigned and the **Checker** drop-down menu must be set to **Cluster Checks**. The GEO LoadMaster polls the connection statistics of the LoadMaster and uses a portion (or all) of the available data to determine the overall level of busyness for the relevant Virtual Service. The site IP address with the lowest load value receives the requests.

This selection criterion is not dependent on the geographical IP database but does require a LoadMaster cluster.

Proximity and Location Based



Location Based load balancing allows GEO to direct a client to a data center based on the client's country, continent or IP address range as defined by the created policies. If there is more than one site with the same country code, requests are distributed in a round robin fashion to each of the sites. **Location Based** load balancing can be used for granularity, for example, if a site in Germany fails – send traffic to the next site in Europe (not the next closest proximity site).

Proximity takes **Location Based** one step further and allows for longitude and latitude granularity for definition of proximity. When using **Proximity** scheduling, new public sites are automatically mapped to geographic coordinates based on the GEO database. New private sites are mapped to 0º0'0" and function as expected. This coordinate should be overridden with accurate values to ensure correct balancing.

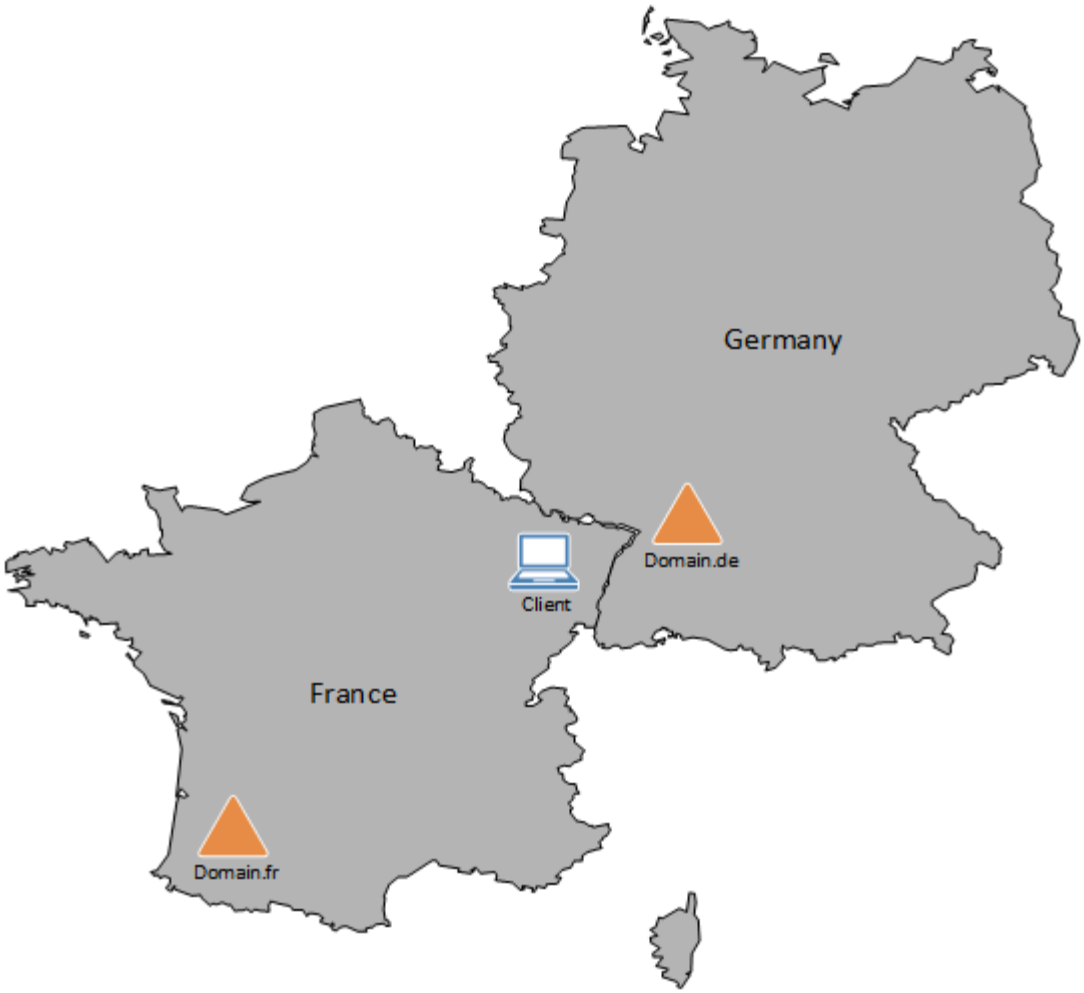
Note: In LoadMaster firmware version 7.2.52, a bug was fixed which had previously caused GEO location coordinates to be changed after creating or modifying an FQDN when using **Proximity** as the **Selection Criteria**. This issue no longer occurs in versions 7.2.52 and above. However, if this issue occurred on a version previous to 7.2.52 and you upgrade to 7.2.52 or above, the coordinates do not get automatically fixed. Therefore, if the incorrect coordinates are already in the LoadMaster, you must manually correct them.

The client source IP address is geocoded in real-time by the LoadMaster then matched against the geocoded longitude and latitude of the cluster or FQDN Real Server definitions. The closest cluster or IP address end-points to the client is the IP address provided to the client. The longitude and latitude of a cluster or IP address end-point is auto-populated and can be manually overridden.

This selection criterion is dependent on the geographical IP database.

To use the **Proximity** selection criteria with private IP addresses, the **IP Range Selection Criteria** must be completed for all private subnets. In addition to this, both the coordinates and country must be configured. If they are not configured, requests from private IP addresses are rejected.

For more information on the **IP Range Selection Criteria**, refer to the IP Range Selection Criteria section.



In the example above, either proximity or location-based scheduling could be used. If proximity scheduling is used, the client is directed towards the German domain because it is geographically closer to it than the

French domain. If location-based scheduling is used, the client is directed towards the French domain because it is in the same country. Using proximity scheduling here may result in a faster connection. However, if users need to be directed towards the French version of a website – it may be better to use location-based scheduling.

All Available

The **All Available** selection criteria returns all possible healthy targets for an A (IPv4) or AAAA (IPv6) query request. The GEO LoadMaster will still refuse other records, for example MX. The contents of the returned list is also controlled by the **Public Requests** and **Private Requests** settings:

- For **Public Sites Only** the list can only contain public addresses. Likewise, for **Private Sites Only** the list can only contain private addresses.
- For **Prefer Public** the list only contains public addresses, unless no public addresses are available – in which case the list contains private addresses (if any are available). Likewise, for **Prefer Private** the list only contains private addresses, unless no private addresses are available – in which case the list contains public addresses (if any are available).
- For **All Sites** the list contains all available addresses

The purpose of this is to provide a list of preferred addresses, if they are available. Otherwise, provide a list of non-preferred addresses as a failback measure for improved availability.

Additional Records



In LoadMaster firmware version 7.2.53, a new **Additional Records** section was added to allow you to configure records for a specific FQDN. You can add, modify, or delete a additional TXT, CNAME, and MX records to an FQDN. These record types allow you to communicate domain resources to clients:

TXT: A TXT (text) record is essentially unformatted data that can be used for almost any purpose, but typically contains information to be consumed by clients to classify a domain in some way, provide details about a domain, or specify resources available within a domain.

CNAME: A CNAME record points a DNS name (such as www.example.com) to another DNS name (such as lb.example.com). This is typically used to define a website alias.

If you select **CNAME** from the **Type** drop-down list, the **NAME** and **RDATA** fields become available. By default, the RDATA field is set with the FQDN name unless some other value is entered in the field. You can add an FQDN that is unrelated to the FQDN to which the records are being added, if desired.

MX: A mail exchanger (MX) record specifies the mail server responsible for accepting email messages on behalf of a domain name.

Note: Underscores are supported in the **Data** field for each of the record types.

The following limits per GEO record and global limits are in place:

- There is a limit of 127 characters in the Data field.
- There is a limit of 64 records of any type per FQDN.

The following validation is in place for CNAME records:

- There cannot be duplicates.
- CNAMEs you add must be part of the domain (must be a child of the FQDN and not the same as the FQDN).
- CNAMEs must be a domain name (no IP addresses).
- FQDNs cannot be added if it already exists as a CNAME.
- Zones cannot be added if it already exists as a CNAME.
- A CNAME cannot be added if an FQDN with the same name already exists.
- A CNAME cannot be added if a Zone with the same name already exists.

For the MX record, there is also a priority. Valid values for the priority field range from 0 to 65535.

The following are not supported as of firmware version 7.2.53:

- Multiple strings within the record: Some DNS providers allow you to put multiple strings in one entry using quotes, for example, "string 1" "string 2" "string 3". Progress Kemp does not allow this as of firmware version 7.2.53, so you can only have "string 1", for example.
- Non-ASCII characters
- Backslashes (\)
- Duplicate records are allowed.

The Time To Live (TTL) value is taken from either the global setting (in **Global Balancing > Miscellaneous Params**) or the local setting in the FQDN (if the **Enable Local Settings** check box is selected).

IP Range Selection Criteria

In the **IP Range Selection Criteria** menu option, you can specify coordinates or a location that apply to an IP address or range. Custom locations can also be added. This allows users to be routed to services based on private IP addresses/ranges as defined manually. It allows the definition of up to 64 IP ranges per data center. The range is limited by the IPv4 or IPv6 native range. You can specify an IP address or network. Valid entries here are either a single IP, for example **192.168.0.1**, or a network in Classless Inter-Domain Routing (CIDR) format, for example **192.168.0.0/24**.

GEO supports subnet precedence for custom-defined IP address ranges in **IP Range Selection Criteria**.

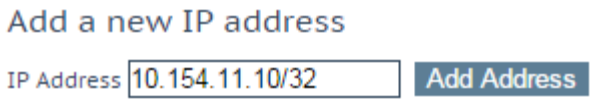
For example:

- 172.16.0.0/12 – United States
- 172.16.100.0/21 – United Kingdom
- 172.16.200.0/21 - Germany

GEO uses the longest prefix for resolution when multiple entries are matched. So, using the example above, 172.16.100.1 should match the /21 United Kingdom resolution rules.

To do this, follow the steps below:

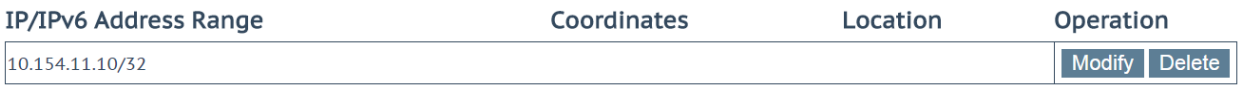
1. In the main menu of the LoadMaster WUI, select **Global Balancing**.
2. Select **IP Range Selection Criteria**.



3. Enter the **IP Address** or network. Valid entries here are either a single IP, for example **10.154.11.10**, or a network in Classless Inter-Domain Routing (CIDR) format, for example **10.154.11.10/32**.

Note: Do not overlap subnets because this can have unpredictable results.

4. Click **Add Address**.

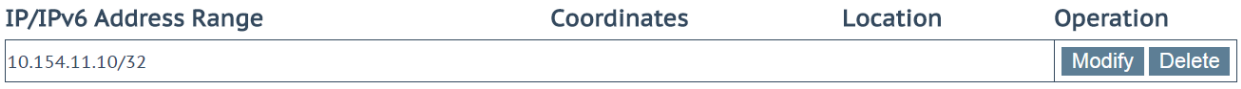


5. Click **Modify**.

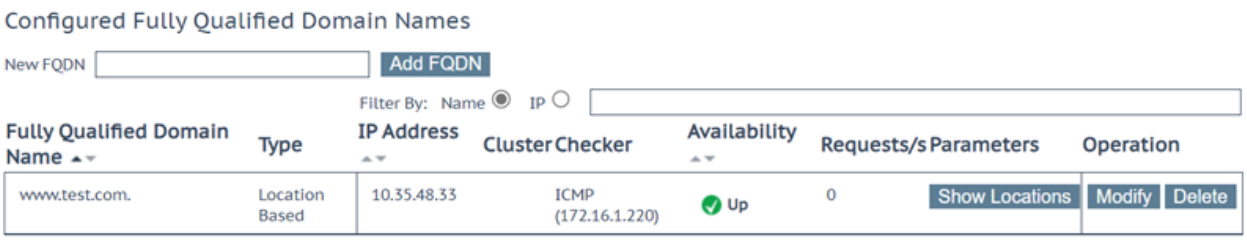


6. Specify the coordinates click **Save**.
7. Alternatively, select the country from the **Location** drop-down list.

Note: The existing IP ranges can be modified or deleted using the buttons provided on the **IP Range Selection Criteria** screen. You cannot delete IP address ranges if they are configured in an FQDN.



8. In the main menu of the LoadMaster WUI, select **Manage FQDNs**.



9. Click **Modify** on the relevant FQDN.



10. If you entered a **Proximity** using the coordinates in the **IP Range Selection Criteria** screen, select **Proximity** in the **Selection Criteria** drop-down list.
11. If you selected a location, select **Location Based**.
12. Fill out the remaining details as needed.

Unanimous Cluster Health Checks

When configuring an FQDN, one of the options which can be configured is **Unanimous Cluster Health Checks**. If this option is enabled, if any IP addresses fail health checking - other FQDN IP addresses which belong to the same cluster is marked as down. When **Unanimous Cluster Health Checks** is enabled, the IP addresses which belong to the same cluster within a specific FQDN are either all up or all down. For example, **example.com** has addresses 172.21.58.101, 172.21.58.102 and 172.21.58.103 which all belong to cluster **cl58**:

- If 172.21.58.101 fails, the unanimous policy forces 172.21.58.102 and 172.21.58.103 down as well.
- When 172.21.58.101 comes back, the unanimous policy brings back 172.21.58.102 and 172.21.58.103 along with it.

At any given time – either all three addresses are available or all three addresses are down.

The same approach applies for site failure mode with manual recovery. Manual recovery causes a failed address to be disabled, so the administrator can re-enable it after fixing the problem. When **Unanimous Cluster Health Checks** is enabled, all three addresses are disabled.

The unanimous policy ignores disabled addresses. So, if you know that an address is down, and for whatever reason you want to continue using the other addresses that belong to the same cluster, you can disable the failed address and the unanimous policy will not force down the other addresses with it.

When **Unanimous Cluster Health Checks** are enabled, some configuration changes may cause FQDN addresses to be forced down or brought back up. For example, if an address is forced down and you remove

it from the cluster while the unanimous policy is in effect, the address should come back up. Similarly, if you add an address to a cluster where the unanimous policy is in effect and one of the addresses is down, the new address should be forced down. This change may not occur immediately, but it should happen the next time health checking occurs.

If there are addresses with the **Checker** set to **None** combined with addresses that have health checking configured – addresses with no health checking will not be forced down, but they can be forcibly disabled if the **Site Recovery Mode** is set to **Manual**. For example, say there are three addresses:

- 172.21.58.101 with a **Checker** of **Cluster Checks**
- 172.21.58.102 with a **Checker** of **Cluster Checks**
- 172.21.58.103 with a **Checker** of **None**

If site failure handling is off or automatic, the failure of 172.21.58.101 causes 172.21.58.102 to be forced down, but 172.21.58.103 remains up. The rationale is that if you do not want health checking on 172.21.58.103 then it should remain up.

However, if the **Site Recovery Mode** is set to **Manual**, failure of 172.21.58.101 causes both 172.21.58.102 and 172.21.58.103 to be disabled, along with 172.21.58.101. For site recovery – all addresses are disabled, even the ones with no health checking configured. This is to keep traffic away from the problem data center until the system administrators fix it. This does not conflict with having addresses with no health checking because you can have an address that is up but disabled.

Manage Clusters

A cluster is a group of LoadMasters working in conjunction. Clusters can also be non-LoadMaster entities using TCP or ICMP health checks. GEO clustering is a feature mainly used inside data centers. Health checks are performed on a machine (IP address) associated to a specific FQDN, using the containing cluster server, rather than the machine itself.

You can add a maximum of 18 GEO clusters.

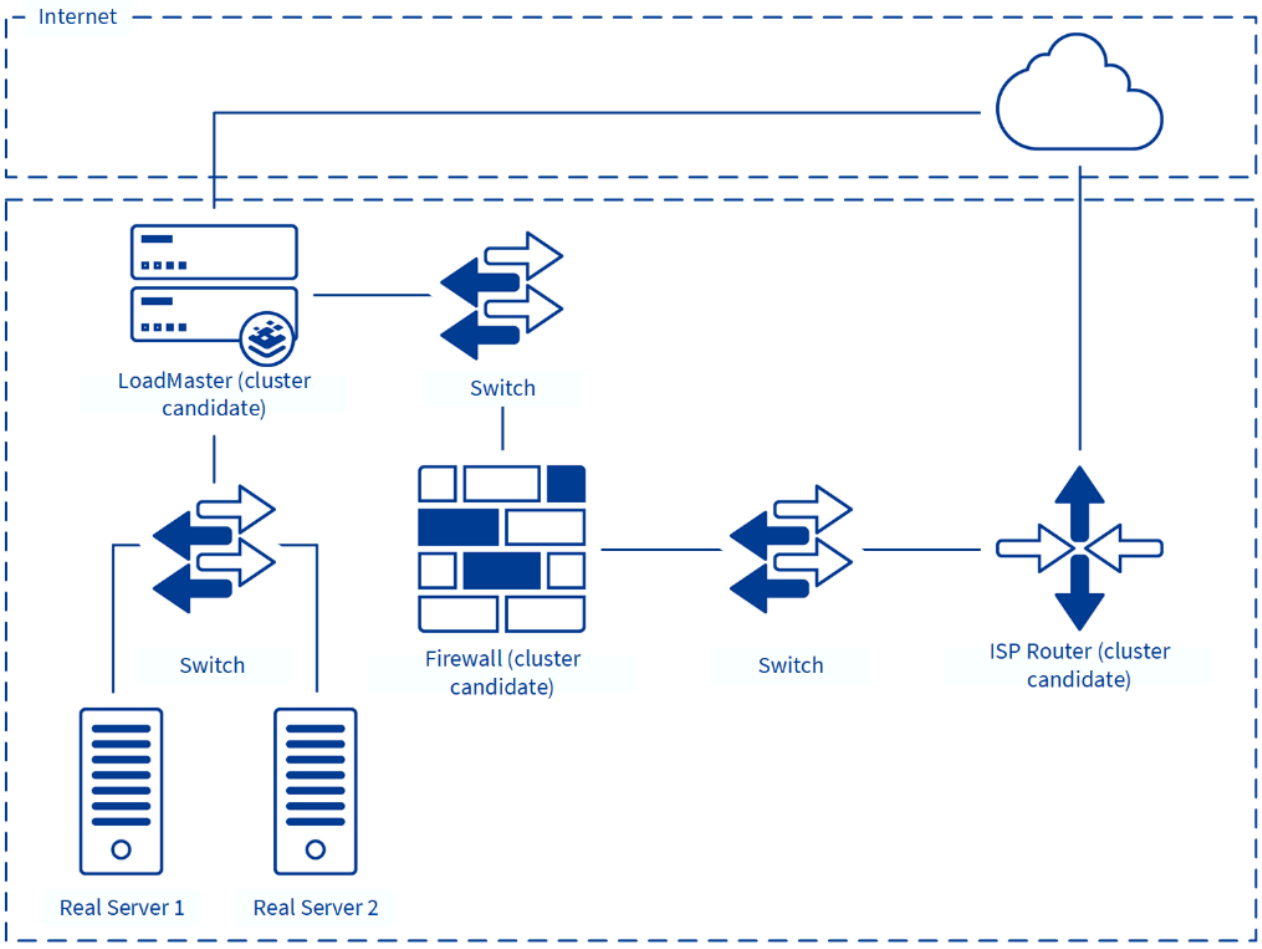
In terms of GEO, a cluster is a GEO LoadMaster polling another device for health checks. For example, a GEO LoadMaster can poll a firewall on a site in front of Real Servers. If the firewall is up, it is assumed that everything behind the firewall is up too. If the health check to the firewall fails, the Real Servers behind the firewall are marked as down.

GEO LoadMasters can be used with a normal LoadMaster as a cluster. There are two methods for clusters:

- First, the LoadMaster can be polled for health checks (same as a firewall or any other device). If this LoadMaster health check fails, everything behind the LoadMaster is marked as down.
- Second, you can use cluster checks. In this case, the GEO LoadMaster polls the LoadMaster and the LoadMaster informs the GEO LoadMaster which Virtual Services are up.

Clusters can be added, modified and deleted from the **Global Balancing** > **Manage Clusters** menu option.

The following diagram helps identify common cluster devices, which include edge routers, firewalls or load balancers. Health checking these devices can summarize the availability of the devices behind their services.



- **ISP Router:** Checking the ISP's edge router will quickly allow the detection of loss of ISP network connectivity
- **Firewall:** Checking the firewall will confirm that the ISP network is available and provides visibility to the first arm of equipment located at the data center
- **LoadMaster:** Checking a load balancer will confirm if the ISP is available, the network infrastructure is available and the Real Servers are responding as expected

Cluster Types

When a cluster is defined, it is possible to set its type. The available cluster types are described below:

- **Default:** When type of cluster is set to **Default**, the check is performed against the cluster using one of the following three available health checks:
  - **None:** No health check is performed. Therefore, the machine always appears to be up.
  - **ICMP Ping:** The health check is performed by pinging against the cluster IP address.
  - **TCP Connect:** The health check is performed by connecting to the cluster IP address on the port specified.

Note: The frequency of the health checks can be specified in the **Miscellaneous Params** screen.

- **Local LM:** When **Local LM** is selected as the **Type**, the **Checkers** field is automatically set to **Not Needed**. This is because the health check is not necessary because the cluster is the local machine.
- **Remote LM:** The health check for this type of cluster is **Implicit** (it is performed by SSH).

Real Server/Cluster Health Checking

GEO utilizes Layer 3, Layer 4 and Layer 7 health checks to monitor the availability of the IP address end-points and clusters. In the case that one of the servers does not respond to a health check within the defined time interval, for a defined number of times, the weighting of this server will be reduced to zero. This zero weighting has the effect of removing the Real Server from the Virtual Service configuration until the Real Server is back online.

Health checks occur from the LoadMaster. Therefore, it is important to make sure that the LoadMaster has access to each cluster and IP address. If all checks fail, ensure that the default gateway is correctly operating.

The following table describes the different health check options available for GEO FQDNs:

Layer	Type	Description
None	None	No check occurs
Layer 3	ICMP	The LoadMaster sends ICMP echo requests (pings) to the Real Servers. An IP address end-point fails this check when it does not respond with an ICMP echo response in the configured response time for the configured number of retries. This is only a relevant health check when the endpoint target is not a LoadMaster.
Layer 4	TCP	The LoadMaster attempts to open a TCP connection to the IP address end-point on the configured service port. The server passes the check if it responds with a TCP SYN ACK in the response time interval. In this case, the LoadMaster closes the connection by sending a TCP RESET. If the server fails to respond within the configured response time

Layer	Type	Description
		for the configured number of times, it is assumed dead.
Layer 7	Cluster Checks	A health check is performed on the IP address of the cluster. Different types of clusters can be defined. The health checks differ for each type: **Default Cluster Type:** An ICMP Ping or TCP Connect health check (depending on what is selected in the **Manage Cluster** options) is performed. **Remote LM Cluster Type:** An SSH connection is attempted. The native LoadMaster statistics are obtained and matched against the FQDN Real Server. If a matching Virtual Service IP is not found, the list of Real Servers cluster is marked as down. Permission to connect must be granted on the LoadMaster. **Local LM:** This method is required if a LoadMaster is co-located with the GSLB Feature Pack for health checks to function correctly. If the **Checker** type is set to **Cluster Checks** and the cluster **Type** (in **Global Balancing > Manage Clusters > Modify > Type**) is set to **Remote LM**, you must also select the associated Virtual Service from the **Mapping Menu** drop-down list. **Note:** If Virtual Services are not displayed in the drop-down list, ensure that both LoadMasters are able to access each other. The remote GEO partner must be configured in **Certificates & Security > Remote Access**. The **Mapping Menu** drop-down list

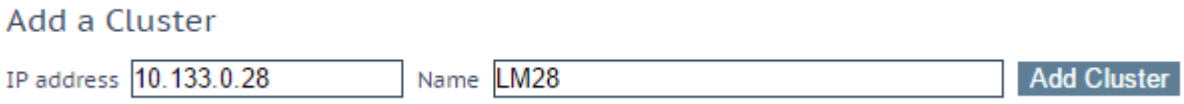
Layer	Type	Description
		displays a list of Virtual Service names (where available) and Virtual Service IP addresses from that LoadMaster. If there are multiple Virtual Services using the same port, there is an entry in the drop-down list for the Virtual Service with up to five ports shown and other individual entries with each port. Select the Virtual IP address and port (or ports) that is associated with this mapping. If a Virtual Service with multiple ports is selected, the health check checks all Virtual Services with the same IP address as the one selected. If one of them is in an “Up” status, the FQDN shows as “Up”. The port does not come in to consideration. If a Virtual Service with one port is selected, the health check only checks against the health of that specific Virtual Service when updating the health of the FQDN.

Add a Cluster

In this example, here are the IP addresses being added:

- GEO LoadMaster: 10.113.0.54
- Regular LoadMaster: 10.113.0.28
- Virtual Service IP address: 10.113.0.37

To add a cluster, follow the steps below on a GEO LoadMaster:



1. Enter the **IP address** of the cluster (in this example it is the LoadMaster with IP address **10.113.0.28**).
2. Enter a **Name** for the cluster.
3. Click **Add Cluster**.

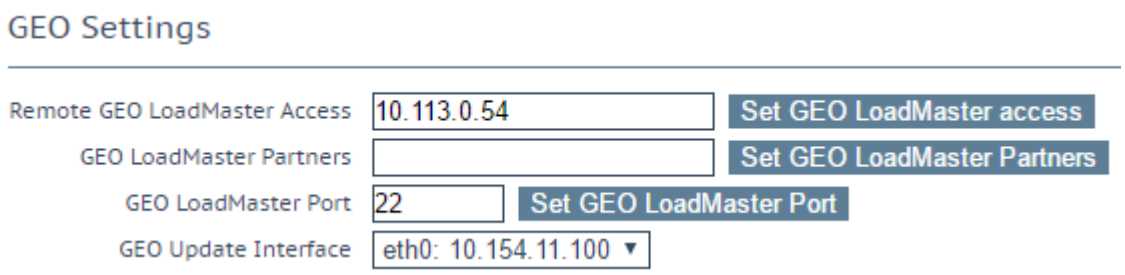
Connect a LoadMaster to a GEO LoadMaster

In the example, the LoadMaster (10.113.0.28) must be connected to the GEO LoadMaster (10.113.0.54). To do this, follow the steps below in the LoadMaster:

1. In the main menu of the LoadMaster WUI, go to **Certificates & Security > Remote Access**.
2. Type a **Partner Shared Secret** and click **Set Secret**.

Note: The **Partner Shared Secret** must match in all units. When an incoming shared secret does not match the local **Partner Shared Secret** (including if only one side is providing a shared secret), a warn-level log message is recorded that says **Unauthorized Remote Machine connection from <ClientIPAddress>** and the connection fails.
This secret must have a minimum of 8 and a maximum of 127 characters. The following characters are supported:

- Numeric: 0-9
- Uppercase alphabetic: A-Z
- Lowercase alphabetic: a-z
- Special characters: !"#$%&()*+,-./:;<=>?[\~]^_@`{|}



3. Type the IP address of the GEO LoadMaster (**10.113.0.54** in this case) and click **Set GEO LoadMaster access**.

Add the FQDN and the Virtual Service IP Address

To add the FQDN and Virtual Service IP address, follow the steps below in the GEO LoadMaster:

1. In the main menu of the LoadMaster WUI, go to **Global Balancing > Manage FQDNs**.

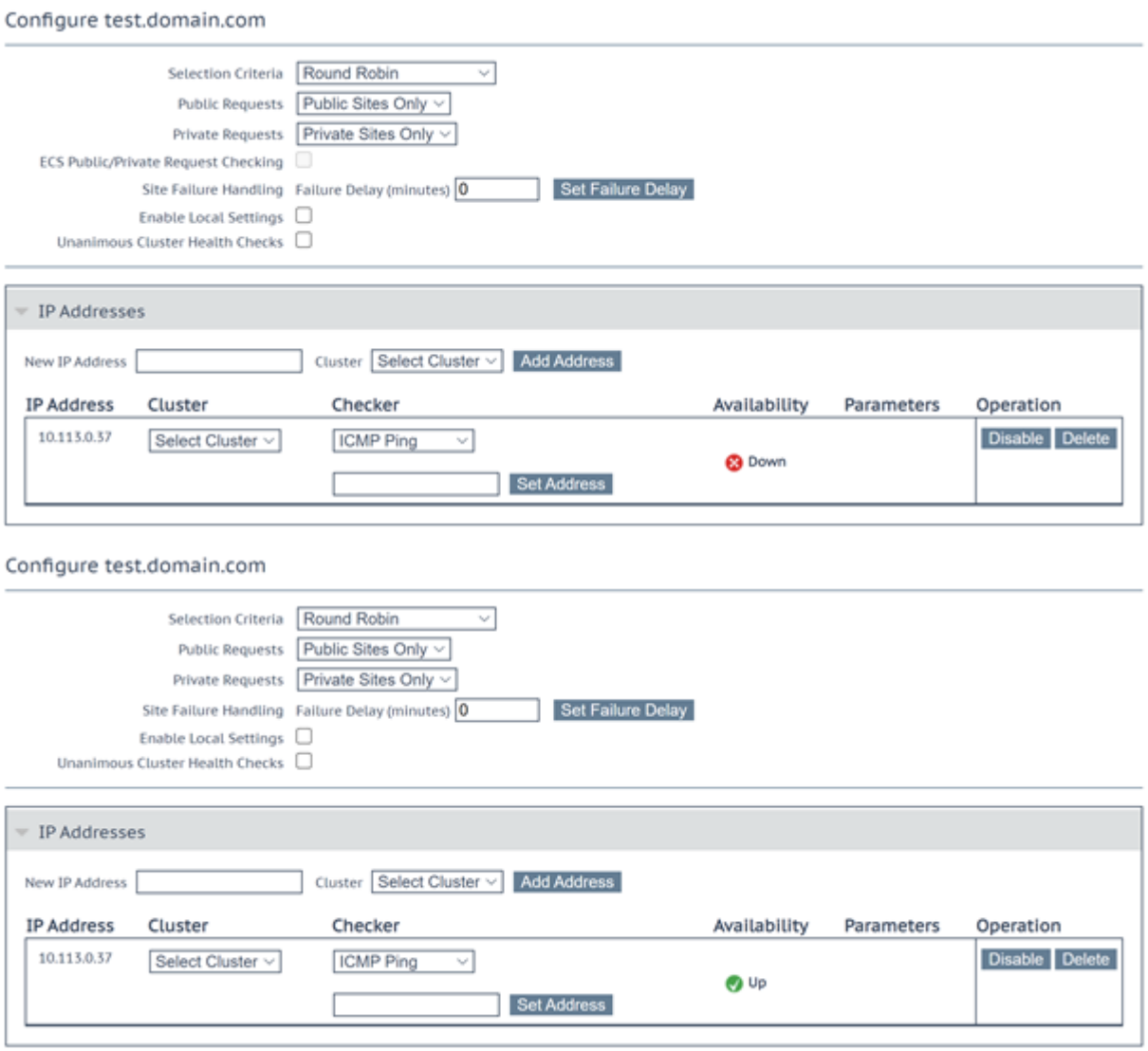


2. Enter the FQDN and click **Add FQDN**.



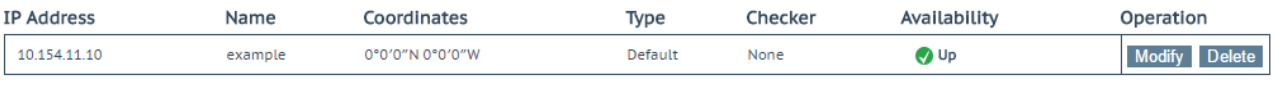
3. Enter the IP address of the Virtual Service (**10.113.0.37** in this example).
4. Select the relevant **Cluster**.

5. Click **Add Address**.



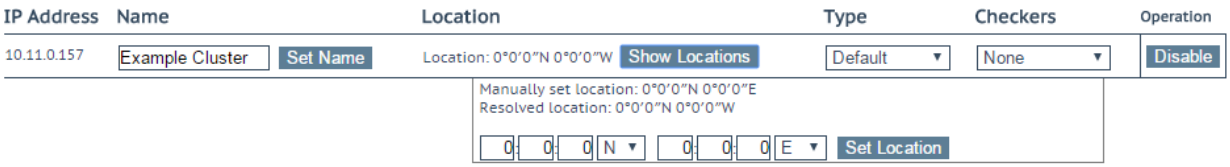
6. Configure any other settings as needed.

Modify a Cluster



To modify an existing cluster, follow the steps below:

1. Click **Modify** on the relevant cluster.



2. Change the settings as needed.

The **Type** can be **Default**, **Remote LM or Local LM**:

- **Default:** When the type of cluster is set to **Default**, the check is performed against the cluster using one of the following three available health checks:
  - **None:** No health check is performed. Therefore, the machine always appears to be up.
  - **ICMP Ping:** The health check is performed by pinging against the cluster IP address.
  - **TCP Connect:** The health check is performed by connecting to the cluster IP address on the port specified.
- **Local LM:** When **Local LM** is selected as the **Type**, the **Checkers** field is automatically set to **Not Needed**. This is because the health check is not necessary because the cluster is the local machine.
- **Remote LM:** The health check for this type of cluster is **Implicit** (it is performed using SSH).

The only difference between **Remote LM** and **Local LM** is that **Local LM** saves a TCP connection because it gets the information locally and not over TCP. Otherwise, the functionality is the same. **Default** is a generic cluster type that does not communicate with a LoadMaster. It uses TCP or ICMP health checks.

Remote LM and **Local LM** are only used when the target is a LoadMaster as opposed to a server or another resource. **Local LM** is used by GEO to check the LoadMaster it is enabled on.

When **Default** is selected, either **ICMP Ping** or **TCP Connect** can be selected as the health check type in the **Checkers** drop-down list.

When **Remote LM** or **Local LM** is selected, no health check options are available. **Remote LM** health checks are performed using SSH on port 22.

If needed, click **Show Locations** to enter the latitude and longitude of the location of the IP address.

Note: After a cluster is initially added, the health check marks it as Up by default. The status is updated after the next health check cycle.

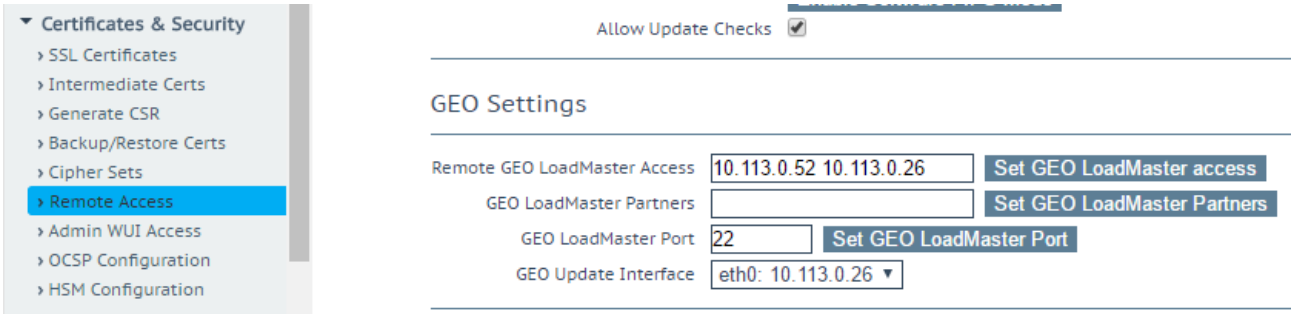
Delete a Cluster

To delete a cluster, click **Delete** in the **Configured Clusters** screen.

Note: There is no “undo” function here. Delete with care.

Clustering Configuration Advice

When setting up clustering in a multi-GEO environment, all LoadMaster clusters must be of the type **Remote LM**.



Each LoadMaster which is to be used as a cluster must have all GEO IP addresses listed in the **Remote GEO LoadMaster Access** field, which is in **Certificates & Security > Remote Access** in the WUI.

When LoadMaster and GEO HA pairs are used, the shared IP address must be listed in the **Remote GEO LoadMaster Access** field.

Configure DNSSEC

DNSSEC verification of signed responses was included in the DNS client in LoadMaster firmware version 7.1.34.

DNSSEC digital signing (2K key) support for DNS responses was added to the GSLB LoadMaster in firmware version 7.2.37.

DNSSEC helps protect against cache poisoning using a set of extensions that provide origin authentication of DNS data, data integrity and authenticated denial of existence. DNSSEC provides a mechanism to sign requests and prove the validity of records in a given zone and does this through a process called zone signing.

DNSSEC adds four new resource record types:

- Resource Record Signature (RRSIG)
- DNS Public Key (DNSKEY)
- Delegation Signer (DS)
- Next Secure (NSEC)

These resource record types are described in RFC 4034.

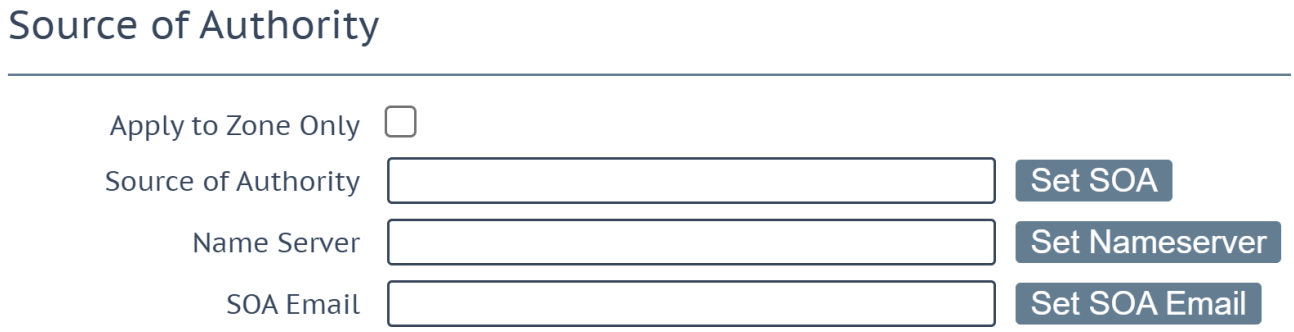
There are also two new DNS header flags, which are:

- Checking Disabled (CD)
- Authenticated Data (AD)

Before configuring DNSSEC, a zone must be defined. You can configure the zone settings in the **Global**

Balancing > Miscellaneous Params screen of the WUI. For further details on the **Miscellaneous Params** screen, refer to the GEO Miscellaneous Params section. A zone is a single unique part of a DNS namespace hierarchy that serves as the authoritative source for information about a select set of DNS domain names.

To group FQDNs within a zone, the FQDN must be the sub-domain of the zone. Otherwise, each FQDN defines a zone.



To define a zone, go to **Global Balancing > Miscellaneous Params** and specify a **Zone Name**.

To enable DNSSEC in the LoadMaster, follow the steps below:

1. Go to **Global Balancing > Configure DNSSEC** to configure the DNSSEC options.



2. You can either import the Key Signing Keys (KSKs), or generate them. To import them, click **Import** and browse to and select the files. If generating, go to the next step.



Note: A KSK is a type of DNSKEY that is used to sign the keys contained within a DNS zone and are leveraged to validate resolvers. The KSK also signs the Zone Signing Key (ZSK).

Note:

If you have GEO partners and want to use DNSSEC, you must generate the KSK files outside of the LoadMaster using the BIND **dnssec-keygen** command and import them onto each GEO partner separately, for example:

```
dnssec-keygen -a RSASHA256 -f KSK -b 2048 -n ZONE <zone_name>
```

Then, import the generated KSK files onto each GEO LoadMaster separately.

3. If generating the KSKs, click **Generate**. Select the **Algorithm** and **Key Size** and click **Generate**.



4. The KSK details are displayed.



5. Select the **Enable DNSSEC** check box.

There is no user interface for ZSK files. A ZSK is used to generate Resource Record Signatures (RRSIG) for each set of resource records in a zone and sign these records. GEO creates the ZSK files automatically when DNSSEC is enabled. The same algorithm is used as specified for the KSK files. A key size of 1024 is used. If DNSSEC is disabled, the KSK files are deleted.

GSLB Statistics

The **GSLB Statistics** screen (accessible from under the **Global Balancing** section in the main menu) is a centralized snapshot of the GSLB components that enable site resiliency and hybrid traffic distribution.



GSLB Service Status

Boot time	Tue, 12 Mar 2019 10:23:13 GMT
Last configuration	Tue, 12 Mar 2019 08:27:38 GMT

FQDN Statistics

Fully Qualified Domain Name	IP Address	Requests/s	Total
www.abhijeettest.com.	1.2.3.4	0	17

Queries

Type	Requests
A	11
AAAA	10
ANY	6

DNS Request Information

Type	Description	Requests
Requestv4	IPv4 Requests Received.	17
Requestv6	IPv6 Requests Received.	10
ReqEdns0	Requests with DNS Extension Mechanisms Received.	7
ReqTCP	TCP requests received.	6
Response	DNS Responses Sent.	27
RespEDNS0	DNS Responses with DNS Extension Mechanisms Sent.	7
QrySuccess	DNS Queries resulted in a successful answer.	17
QryAuthAns	DNS Queries resulted in authoritative answer.	27
QryNxrrset	DNS Queries resulted in NOERROR responses with no data.	10
QryUDP	UDP queries received.	21

The following sections display on the **GSLB Statistics** screen:

- **GSLB Service Status:** Displays the **Boot time** (the start time of the bind device) and the **Last configuration** (the date and time when the configuration was last modified).
- **FQDN statistics:** Displays the FQDN configuration with IP address information.
- **Queries:** Displays the different DNS query types received.
- **DNS Request Information:** Displays the type of DNS requests with a description and request count.

Note: If you disable and re-enable GSLB, the GSLB statistics reset to zero.

Remote Administration

Full remote administration occurs over HTTPS using the default 443 SSL port. Limited remote administration can be performed over SSH using the default port 22. This includes system level configuration, debugging/ advanced troubleshooting but not DNS administration. The recommended graphical user interface for remote administration is HTTPS.

When negotiating a HTTPS connection with the LoadMaster you may be required to acknowledge security warnings, for example, acknowledging a discrepancy between the hostname and IP or the signer of the certificate. It is safe to allow/permit overrides, all LoadMaster occurs over a secure channel regardless of these warnings. To permanently remove the warning about signing authority you can download the Root certificate by clicking **Download Root Cert** in the main menu.

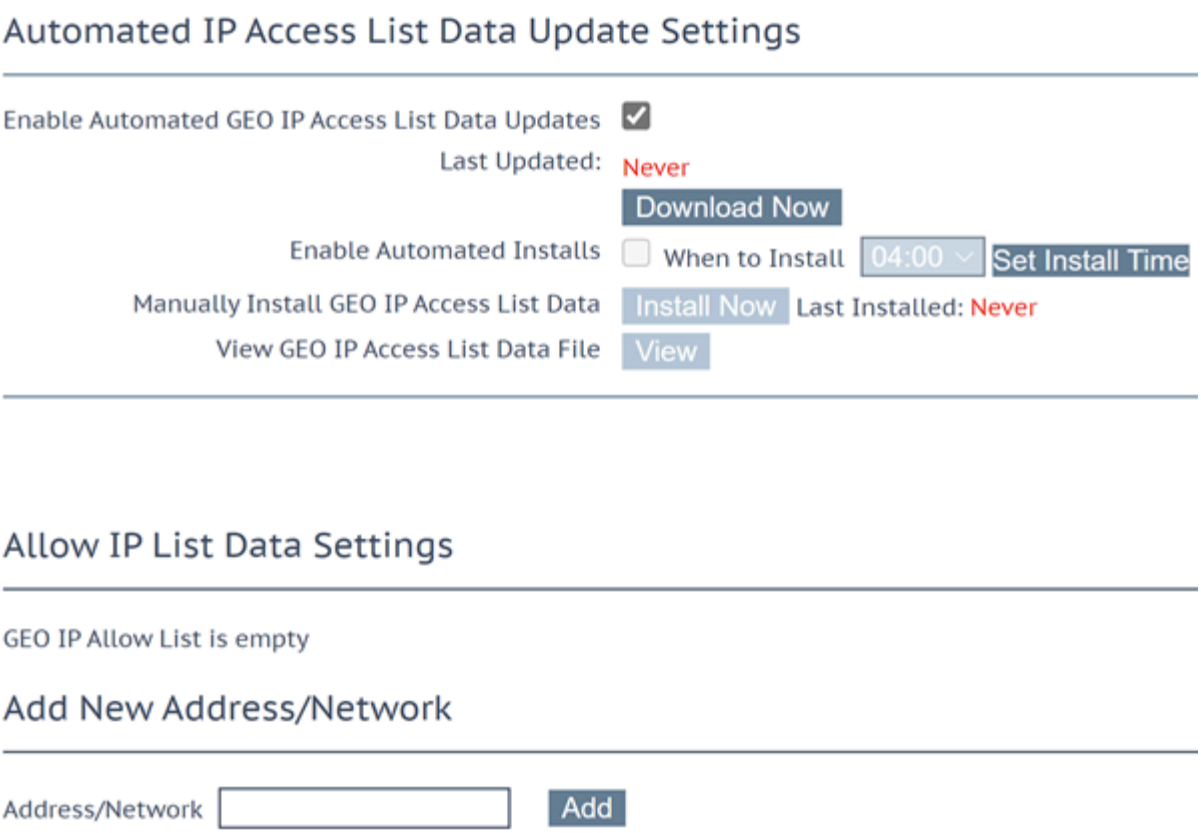
IP Access List Settings

It is possible to download access-list rules from Progress Kemp to block access from IP addresses that are on the access-list. An allow list can be manually specified that overrides the access-list. These rules can be set to automatically download and install or they can be manually downloaded and installed.

Note: This is a subscription-based feature. If you cannot see these options, or if any fields are grayed out, please contact Progress Kemp to upgrade your subscription.

To configure the IP access-list settings, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Global Balancing > IP Access List Settings**.



2. Either enable or disable the **Enable Automated GEO IP Access List Data Updates** check box.
3. In the **Last Updated** section, you can manually download the rule updates now. You can also view changes, that is, what are the differences between the latest downloaded rules and the previously downloaded rules.

Note: After downloading the rule updates, they must be installed to become active. If the rules are more than 7 days old, a message appears.

---

4. Either enable or disable the **Enable Automated Installs** check box. When enabled, you can specify what time to install the updates at.

Note: When the **Enable Auto-Save** option (under **System Configuration > Miscellaneous Options > WUI Settings**) is enabled and you select a new hour value, the value gets auto-updated.

When the **Enable Auto-Save** option is disabled, you must click **Set Install Time** after selecting a new hour value to update the installation time. If the hour value in the drop-down list has not been changed from its previous value and you click **Set Install Time**, the following error message displays:

"Value has not been changed. If auto-save is disabled, select a new value and press the set button again."

---

5. You can Manually Install the GEO IP access-list data by clicking **Install Now**.

Note: If the GEO access-list data is not updated for more than 7 days, a message appears.

---

6. View the GEO IP access-list data file by clicking **View**. This displays a full list of the blocked IP

addresses.

7. Addresses and networks can be added to the allow list by entering them into the **Address/Network** text box and clicking **Add**. The allow list overrides the access-list.

Certificates

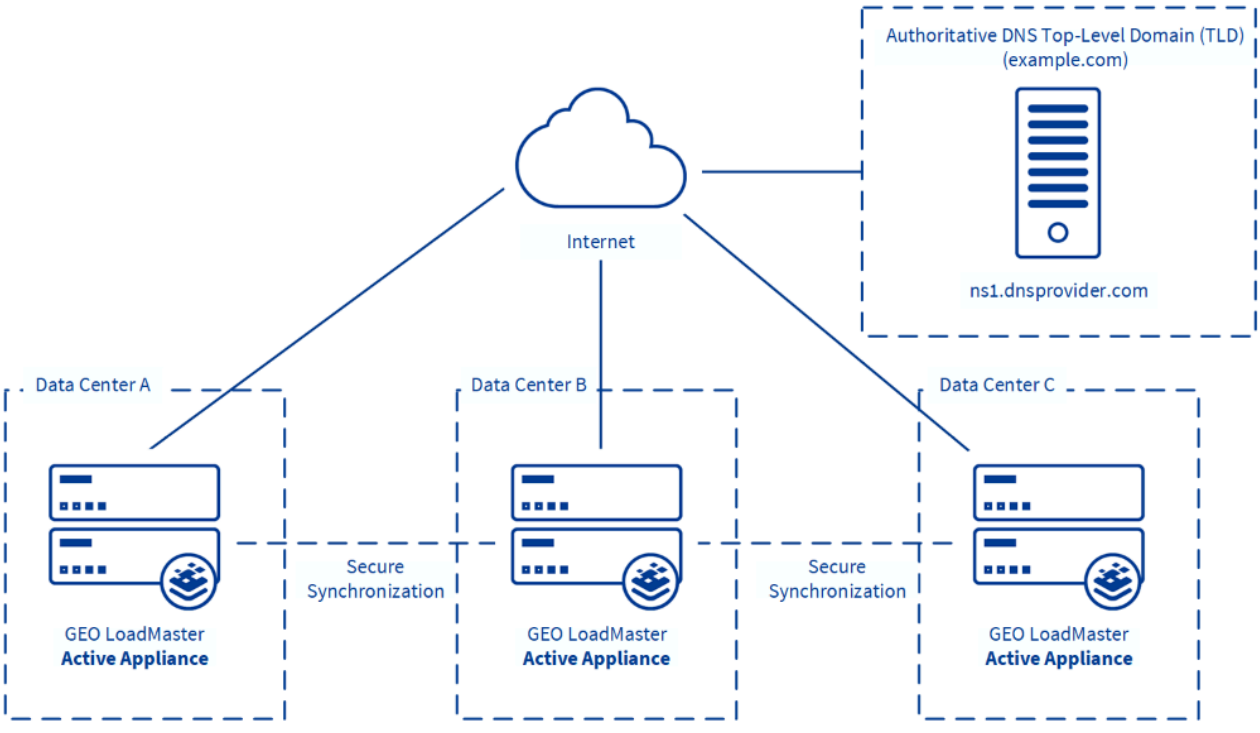
The **Certificates & Security** option in the main menu of the LoadMaster WUI enables you to import and manage SSL certificates. It also gives the ability to generate a Certificate Signing Request (CSR). This option is only relevant for the GEO LoadMaster WUI access.

Distributed LoadMaster Partners

When there are multiple LoadMaster boxes, where each box could be a single LoadMaster or a HA pair, they can be linked together to act as a single resource.

Note: When a HA LoadMaster pair is configured to do GEO synchronization, all of the shared IP addresses must be added to each partner configuration correctly.

All of the boxes remain synchronized with each other and share their DNS Configurations, FQDN information, 'Stickiness' information and health checking updates. Any updates are automatically shared with all the other Distributed Partners.



Note: The Geographical IP Database used for the **Proximity** and **Location Based** load balancing methods

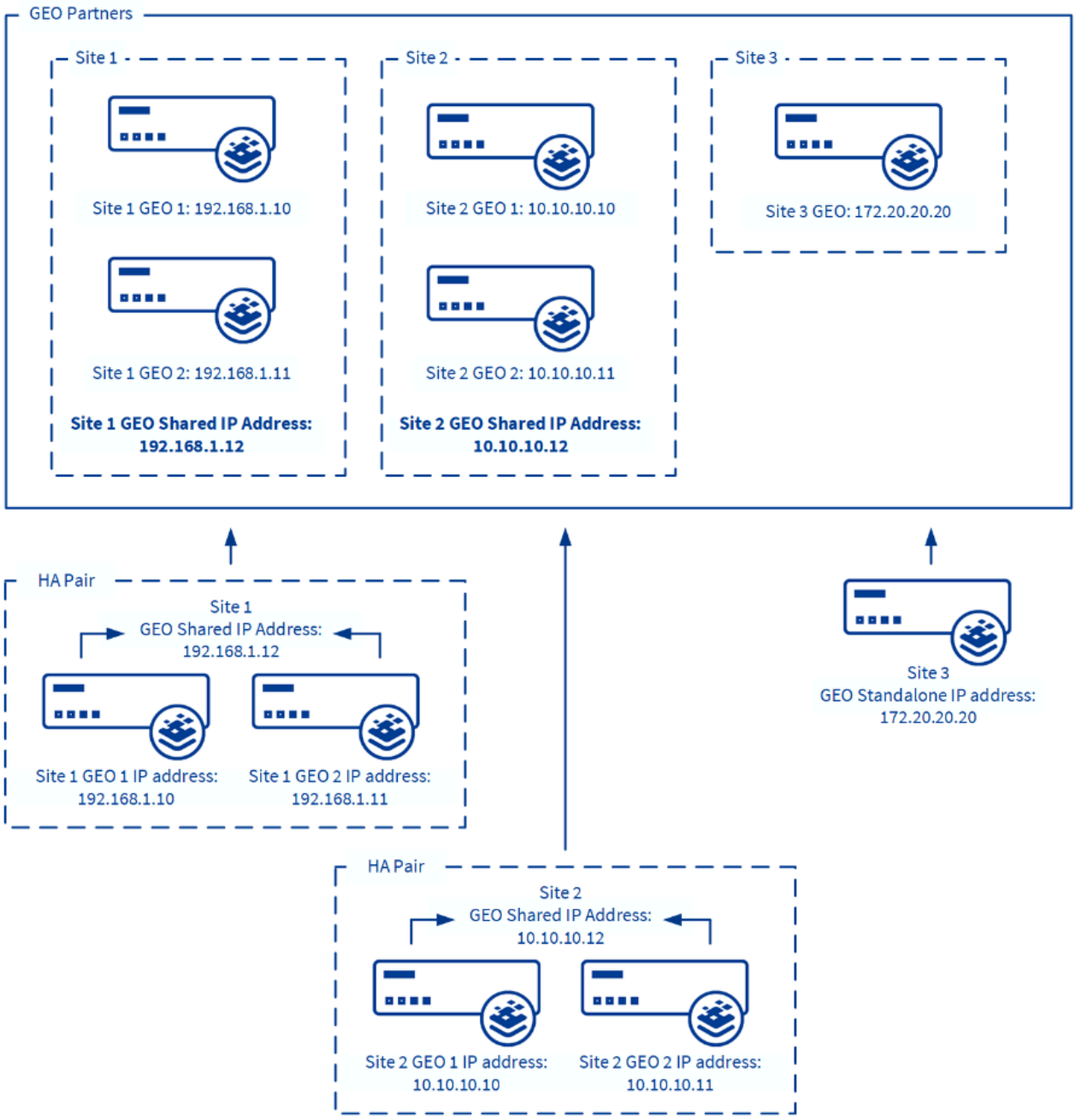
is not distributed between the LoadMaster partners. Any updates to the Geographical IP Database must be configured on each LoadMaster individually.

HA Versus Partners

HA is the same for GEO LoadMasters as it is for regular LoadMasters – it is an active-passive pair of units.

Partners are two or more GEO units in an active-active mode.

It is possible to have both HA and partners.



In the example diagram above, public and private addresses are used. The partner address should be the NATed addresses if the GEOs are connecting externally.

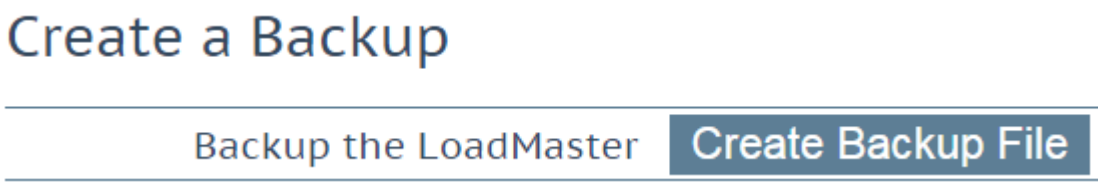
Set Up GEO LoadMaster Partners

Before partnering GEO LoadMasters, backup the relevant GEO LoadMaster that has the correct/preferred configuration. This backup should then be restored to the other LoadMasters that are partnered with the original LoadMaster. This is a prerequisite because GEO partners are active-active and share the same configuration. As a result of this, you must ensure that the settings are in sync before adding a partner.

Backup and Restore the Correct Configuration

To perform a backup, follow the steps below in the WUI of the GEO LoadMaster that has the correct/ preferred configuration settings:

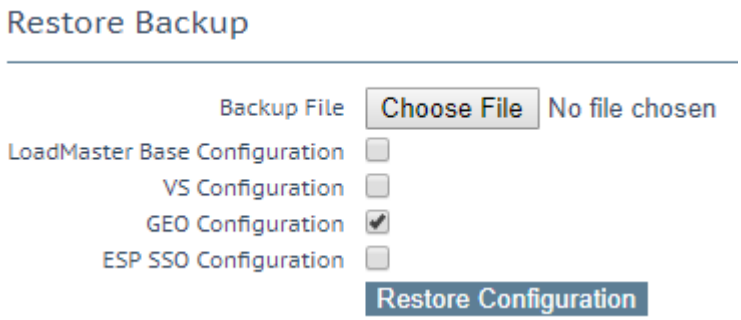
1. In the main menu, go to **System Configuration > System Administration > Backup/Restore**.



2. Click **Create Backup File**. The file downloads.

   Then, on the GEO LoadMaster(s) that are partnered - follow the steps below to restore the configuration:

3. In the main menu, go to **System Configuration > System Administration > Backup/Restore**.



4. Click **Choose File**.
5. Browse to and select the backup file.
6. Select the **GEO Configuration** check box.
7. Click **Restore Configuration**.

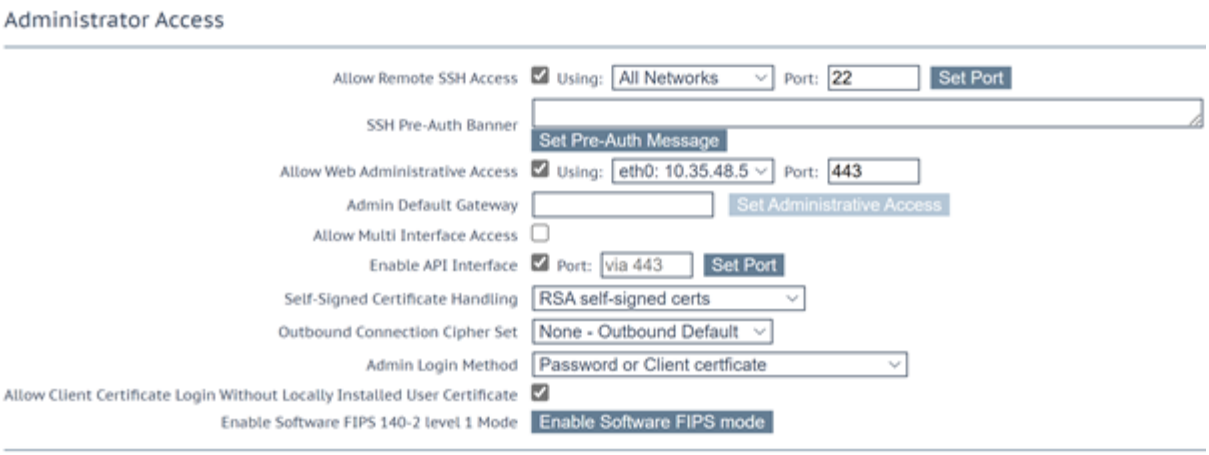
Now that the correct configuration is applied, the GEO LoadMasters can be partnered.

Partner the GEO LoadMasters

When configuring two GEO units as partners, the communication between the two units occurs through the **Admin Default Gateway** if one is configured on the **Certificates & Security > Remote Access** page. Otherwise, communication occurs through the system **Default Gateway** on the **System Configuration > Network Setup > Default Gateway** page. If this behavior does not match the needs of your configuration, a static route can be created to send partner responses out of the required interface.

To partner the GEO LoadMasters, follow the steps below:

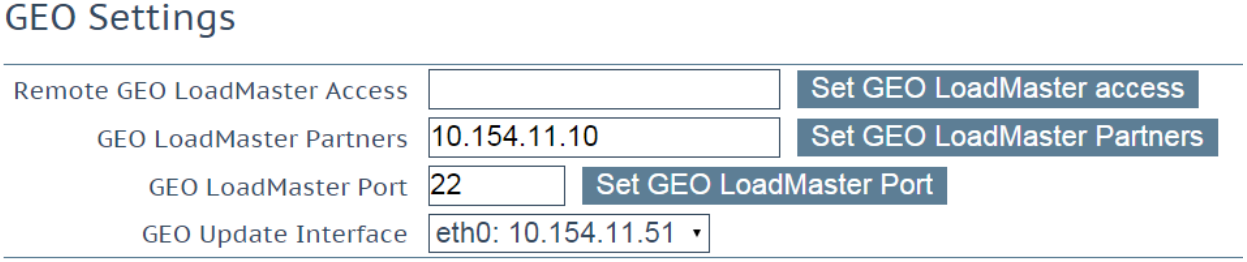
1. Select the **Certificates & Security > Remote Access** option from the main menu.



2. Ensure the **Allow Remote SSH Access** check box is selected.
3. Enter a **Partner Shared Secret** and click **Set Secret**.

Note: The **Partner Shared Secret** must match on all GEO partners. When an incoming shared secret does not match the local **Partner Shared Secret** (including if only one side is providing a shared secret), a warn-level log message is recorded that says **Unauthorized Remote Machine connection from <ClientIPAddress>** and the connection fails.
This secret must have a minimum of 8 and a maximum of 127 characters. The following characters are supported:

- Numeric: 0-9
- Uppercase alphabetic: A-Z
- Lowercase alphabetic: a-z
- Special characters: !"#$%&()*+,-./:;<=>?[\~]^_@`{|}



4. In the **GEO LoadMaster Partners** text box, enter the IP address of the LoadMaster to partner with. If there is more than one box, enter the IP addresses but separate them with a space.

Note: The maximum number of GEO partners allowed is 64.

---

5. Click **Set GEO LoadMaster Partners**.
6. Enter the port number that the LoadMasters use to communicate in the **GEO LoadMaster Port** text box.
7. Click **Set GEO LoadMaster Port**.
8. In the **GEO update interface** drop-down list, select the GEO interface that the GEO partners will communicate through.
9. Repeat the above steps for all other GEO LoadMasters to be partnered.

GEO Partners Status

After a GEO LoadMaster is partnered, its status is indicated in the **GEO Partners** section of the **Remote Access** screen.

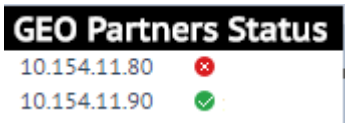


Figure 3-22 shows GEO Partner status of **Green** indicating the two partners can see each other.

Figure 3-22 also shows GEO Partner status of **Red** indicating the LoadMasters cannot communicate. The reasons for this include (among other possibilities); one of the partners is powered down, there may be a power outage or a cable disconnected.

A red status could also appear because when initially set, the status of the GEO Partner on the first GEO LoadMaster displays as red. When you set the GEO Partner on the second GEO LoadMaster, the status displays as green on the second LoadMaster but remains red on the first GEO LoadMaster for approximately three minutes until the first GEO LoadMaster updates. As a workaround, click **Set GEO LoadMaster Partners** on the first LoadMaster again and the status changes to green.

If there is a failure to update the GEO partner, the logs display an error message saying the GEO update to the partner failed. The message displays the IP address of the partner.

If you experience any issues with partnering the GEO LoadMasters, check the SSH settings and do a TCP dump to confirm that SSH connections are being sent and received by all parties.

Upgrading GEO Partners

When upgrading GEO partners, it is strongly recommended that all nodes are upgraded simultaneously. Because GEO partners operate in active-active mode, upgrading at the same time ensures that consistent behavior is experienced across all nodes.

If you must operate a GEO cluster with mixed versions, be sure to make all changes from the most recent version. This prevents configuration loss due to incompatible configurations. Additionally, changing configuration options not present in older versions results in disparate behavior.

Configuring GEO for Exchange Site Resiliency

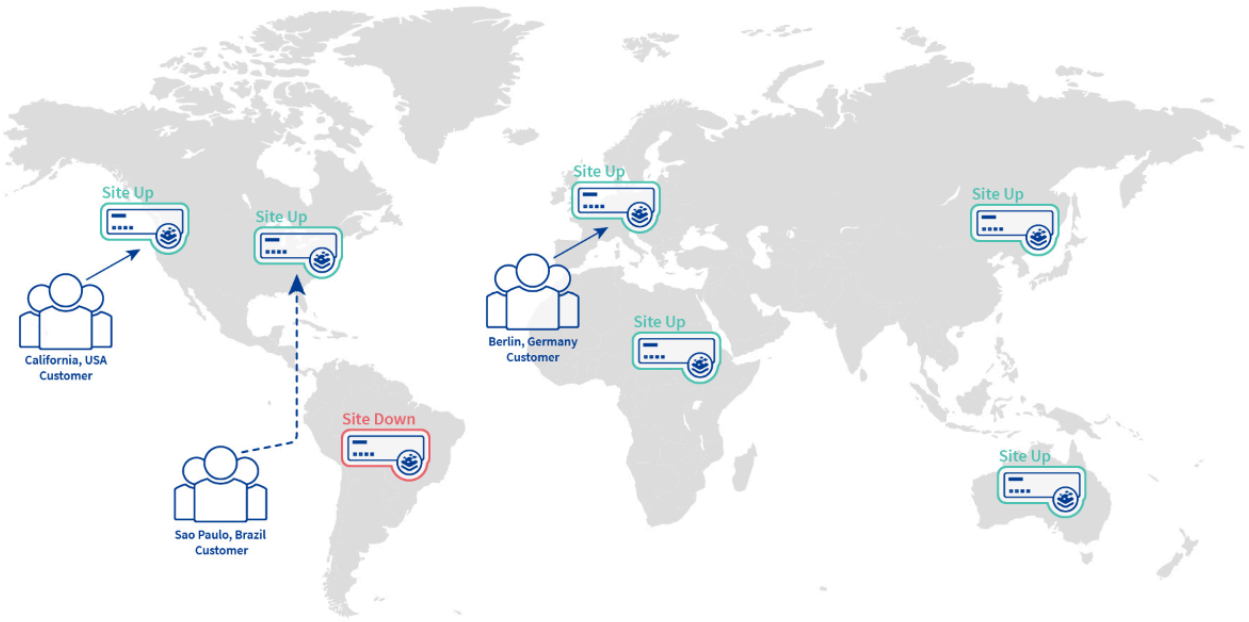
Configuring GEO for Exchange Site Resiliency

Microsoft Exchange data center or site failures require a combination of both automatic and manual steps to be completed before client service is fully restored and for the outage to end. The manual steps, mainly centred on the administration of the mailbox databases, pose some unique issues regarding an Exchange data center failover which are not found in other types of site failures.

GEO functionality provides options to Exchange administrators to assist in dealing with the unique issues posed by an Exchange data center failover.

Enabling Fail Over

Enabling Fail Over



We recommend enabling the **Fail Over** option in Exchange environments.

Enabling the **Fail Over** option enables **Location Based** FQDNs to select the most appropriate site for requests in the event that the best match is not available. When the **Fail Over** option is enabled, if a request comes from a specific region and the target is down, the connection will fail over and be answered with the next level in the hierarchy. If this is not available, the connection is answered by the nearest (by proximity) target. If this is not possible, the target with the lowest requests are picked. For example, if a request from Ireland is received, but the site assigned to **Ireland** is unavailable, a site assigned to **Europe** is selected. If the site assigned to Europe is also unavailable, a site assigned to **Everywhere** is selected. If this too is unavailable, the site with the lowest requests of the available sites in the same continent is selected using the round robin method. The **Fail Over** setting affects all targets. The **Fail Over** option is only available when the **Selection Criteria** is set to **Location Based**.

Fail Over is set on all GEO nodes. If a partner GEO unit has been configured, you can assume that all nodes are operating on the same configuration. The settings in one GEO is synced to all other GEO nodes.

Delaying a Failover

Delaying a Failover

By default, if a target is unavailable (that a request would typically be directed to) - that is, the server is down - the request is directed to the next best available alternative target. When the original target becomes available, it is set into rotation after the specified timeout or failover. However, if needed it is possible to set a

Failure Delay. **Failure Delay** is very important in Exchange data centers.

Implementing an Exchange data center failover is not a trivial event - it is not recommended to automatically failover upon detection of a site failure. Delaying the failover for a short period ensures that failovers do not occur because of trivial and temporary failures.

Delaying the failover can also provide the Exchange administrators time to ensure that the secondary site is ready to provide the requisite levels of service.

The LoadMaster provides a **Failure Delay** option which, when enabled, delays a failover occurring for a configurable period of time after a site failure is detected. If, after the delay, the site recovers, the failover is not initiated. If the site has not recovered, the failover is initiated as per normal.

If a **Failure Delay** is set, another option becomes available underneath it – **Site Recovery Mode**. If an endpoint fails the health check it is marked as "failing". After the **Failure Delay** time ends, the endpoint is marked as down. The **Site Recovery Mode** determines what recovery options are implemented when a failed site recovers.

- **Automatic** - when the endpoint recovers (passes the health check), the endpoint is marked as up and the LoadMaster automatically makes the endpoint available for use
- **Manual** - upon failure, the endpoint is administratively disabled and is not available for use until you click **Enable** for the relevant endpoint and the health check is passing.

Requiring Manual Intervention Before Failback Occurs

Requiring Manual Intervention Before Failback Occurs

It is recommended that when a failed data center recovers, attempting to restore services to the recovered data center is not initiated (a failback) before the application failover process is complete and until the recovered data center is deemed to be healthy. In addition, the mailbox databases should beready for use.

If the failback is initiated before these are complete, then issues may arise with the mailbox databases and prolong the outage.

We recommend not allowing automatic failbacks when a failed data center recovers in the case of Microsoft Exchange. Requiring some manual intervention before a recovered data center is deemed available for a failback means that administrators can ensure that the optimal conditions exist before a failback occurs.

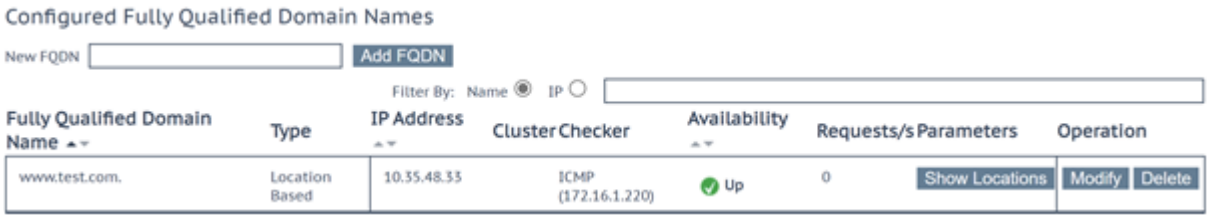
The LoadMaster provides Site Recovery Mode options that determine how a failed data center becomes available for failback upon recovery. Selecting the manual option configures the LoadMaster to administratively disable the failed data center upon the initiation of a failover. This ensures that, even if the failed data center recovers, administrator intervention would be required before the data center is available for a failback to occur.

Configuring Site Resiliency Options for Exchange (Example Configuration)

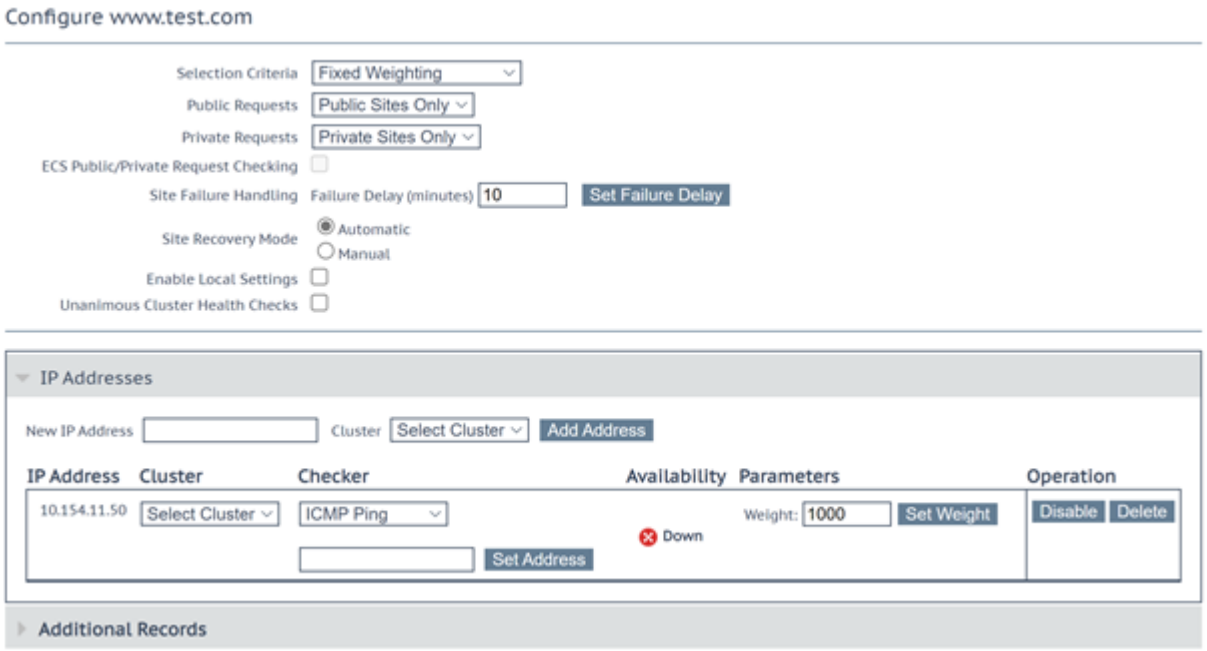
Configuring Site Resiliency Options for Exchange (Example Configuration)

GEO functionality provides options to Exchange administrators to assist in dealing with the unique issues posed by an Exchange endpoint failover. These options can be found within the **Site Failure Handling** section of the FQDN configuration page, which is accessed as follows:

1. In the main menu, go to **Global Balancing > Manage FQDNs**.



2. Click **Modify** for the relevant FQDN.



Failure Delay

This setting determines how long (in minutes) the LoadMaster waits until it designates a site as having failed, thereby initiating a site failover.

It is recommended that this setting is enabled when configuring multi-site Exchange deployments. The optimal value given to the delay depends on the configuration of the Exchange deployment.

Site Recovery Mode

The **Site Recovery Mode** options only become available when a **Failure Delay** is set. The **Site Recovery Mode** determines what recovery options are implemented when a failed site recovers.

- **Automatic** - when the endpoint recovers (passes the health check), the endpoint is marked as up and the LoadMaster automatically makes the endpoint available for use
- **Manual** - upon failure, the endpoint is administratively disabled and is not available for use until you click **Enable** for the relevant endpoint and the health check is passing.

The **Manual** option is recommended for multi-site Exchange deployments to ensure that failbacks do not occur until the administrators ensure that the optimal conditions for a failback exist.

5

Troubleshooting

Troubleshooting

Refer to the following sections for troubleshooting information relating to persistence/stickiness and scheduling.

Related Links

For details, see the following topics:

- Persistence/Stickiness
- Scheduling

Persistence/Stickiness

Persistence/Stickiness

If connecting from a client to the GEO LoadMaster directly the GEO LoadMaster keeps a persistence entry for the request. If connecting from a DNS server to the GEO LoadMaster directly, the GEO LoadMaster keeps a persistence entry for the request as does the DNS server. For troubleshooting, ensure to set stickiness on the GEO LoadMaster to **0** and clear the DNS cache on the DNS server.

To clear the DNS cache on a Windows server, run the following command:

```
c:\> Dnscmd  /clearcache
```

Always test with the **nslookup** command or the **dig** command directly against the GEO LoadMaster to confirm the results.

Scheduling

Scheduling

Round Robin

This is the same principle as the normal LoadMaster with one exception - when using the **nslookup** command, by default, it checks for both IPv4 (A) records and IPv6 (AAAA) records, which actually sends out two requests.

If you have two sites:

- Request 1 - IPv4 A round robin to Site 1
- Request 2 - IPv6 AAAA round robin to Site 2
- Request 3 - IPv4 A round robin to Site 1
- Request 4 - IPv6 AAAA round robin to Site 2

When testing, clients looking for IPv4 always connect to Site 1 and clients looking for IPv6 always connect to Site 2. To help prevent this from occurring during testing, you can add an odd number of sites.

nslookup Troubleshooting

nslookup command:

```
c:\> nslookup <FQDN> <GEO address>
```

For example:

```
c:\> nslookup geotest.lan 10.113.0.52
```

```
C:\>nslookup geotest.lan 10.113.0.52
Server:  UnKnown
Address:  10.113.0.52

Name:    geotest.lan
Address:  10.10.10.10
```

Response is:

```
Name: geotest.lan

Address: 10.10.10.10
```

Commands for further testing:

Changes request type to IPv4 A record:

```
nslookup –query=A
```

Changes request type to IPv6 AAAA record:

```
nslookup –query=AAAA
```

DIG command:

```
user@linux: dig <domain>
```

```
user@linux: dig test.domain.com
```

Search for an FQDN:

```
user@linux: dig –t <record type> <FQDN>
```

```
user@linux: dig –t A test.domain.com
```

Search for an **A** record type:

```
user@linux: dig –t <record type> <FQDN>
```

```
user@linux: dig –t AAAA test.domain.com
```

Search for an **AAAA** record type:

```
user@linux: dig –t A <DNS server/ GEO> <domain>
```

```
user@linux: dig –t A @10.113.0.54 test.domain.com
```

Search for an **A** record type against this DNS server or GEO (10.113.0.52).

6

References

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/:

Web User Interface (WUI), Configuration Guide

GEO Sticky DNS, Feature Description

SSL Accelerated Services, Feature Description

Web Application Firewall, Feature Description