GEO

Product Overview

VERSION: 9.0

UPDATED: July 2017

Copyright Notices

Table of Contents

1 Introduction

GEO assures seamless failover and failback to the best performing and geographically closest datacenter for optimal use of web-based applications, including Microsoft Exchange. In the event of a service disruption, traffic is automatically controlled based on a set policy in order to minimize impact and the need for manual intervention.

The GEO product is available in two forms:

- A standalone GEO product
- A Global Sever Load Balancing (GSLB) Feature Pack that is part of the KEMP LoadMaster product

Throughout this document, when we refer to the "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 KEMP's Server LoadMaster hardware 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 can occur at the services level or even the site level, allowing for flexible decision making on when traffic should be diverted per Fully Qualified Domain Name (FQDN).

GEO offers many load balancing algorithms including **round robin**, **weighted round robin**, **fixed weighting**, **real server load**, **location based** and **proximity**. "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. **Location Based** load balancing allows GEO to direct a client to a data center based on the client's country or continent, as defined by the created policies. **Proximity** takes **Location Based** one step further and allows for longitude and latitude granularity for definition of proximity. GEO securely and seamlessly integrates with LoadMaster to offer "Real Server Load" load balancing, in which GEO uses local data center metrics provided by LoadMaster, allowing clients to connect to the least busy data center.

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

1.1 Document Purpose

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

1.2 Intended Audience

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

2 GEO Overview

An overview of the GEO product and functionality can be found in the sections below.

2.1 High Availability (HA)/Reliability

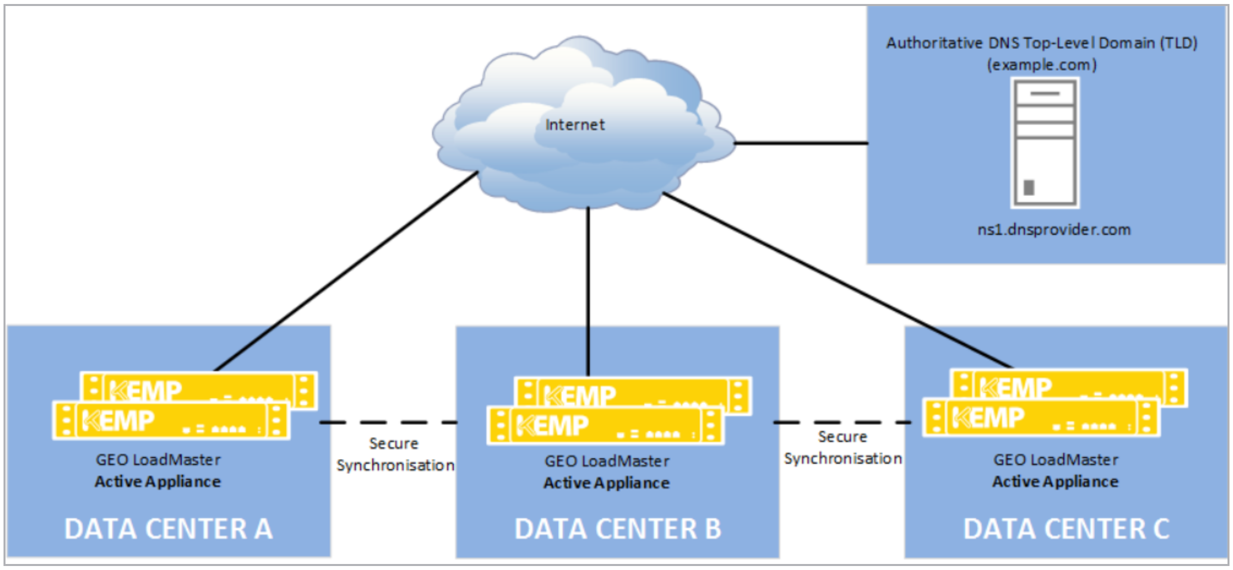
GEO helps optimize data center functionality through client request distribution and prevent service outages by quickly detecting data center resource failures and then directing traffic accordingly. Monitoring and load balancing are based on layers 3 and 4 of the Open Systems Interconnection (OSI) Basic Reference Model. Included in HA is the ability to have multiple LoadMasters, protecting against single points of hardware or network connectivity failure. Each individual KEMP LoadMaster can also be configured to provide network link-layer redundancy.

2.2 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.

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.



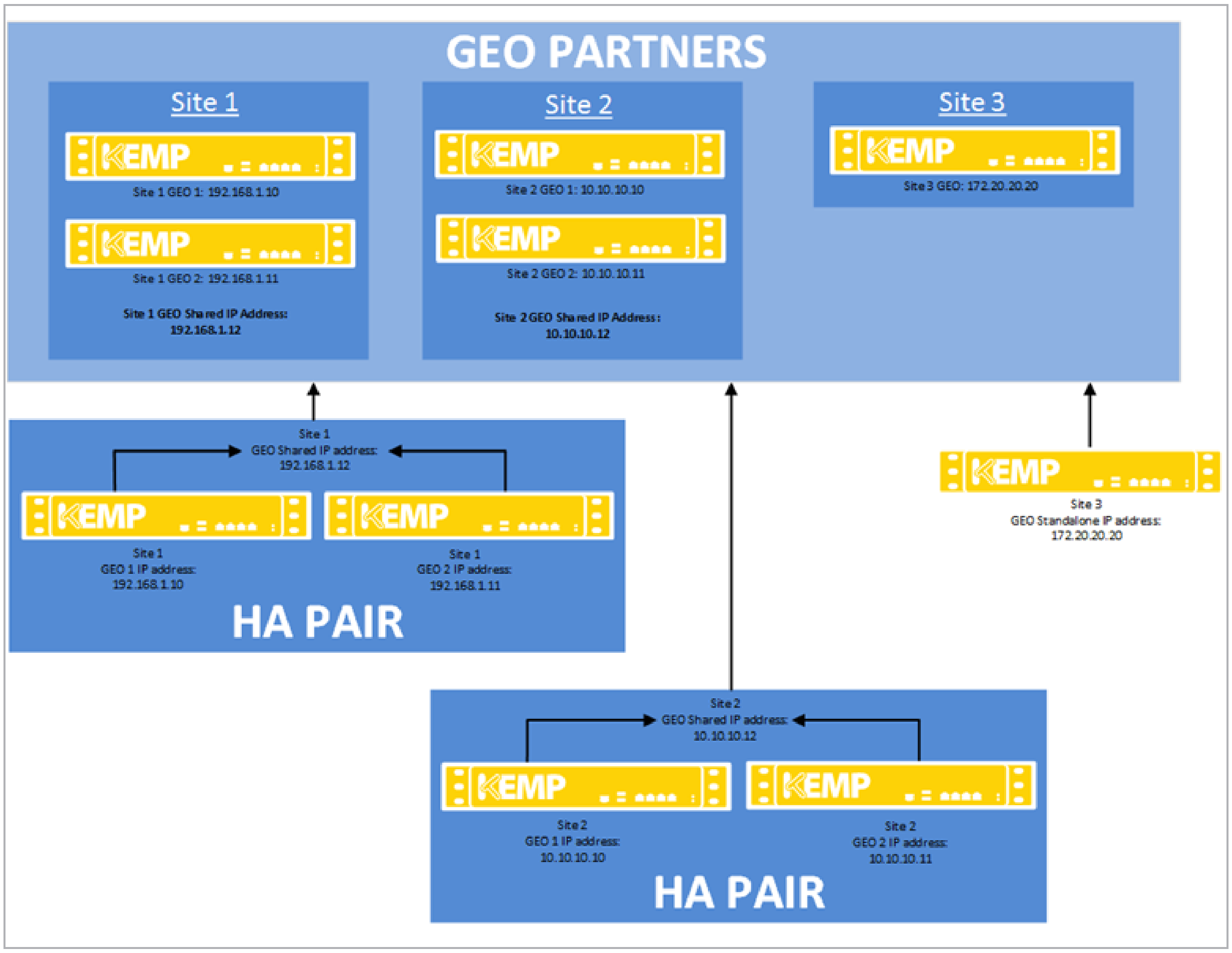
The Geographical IP Database used for the Proximity and Location Based load balancing methods is not distributed between the LoadMaster partners. Any updates to the Geographical IP Database must be configured on each LoadMaster individually.

2.2.1 HA Versus Partners

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

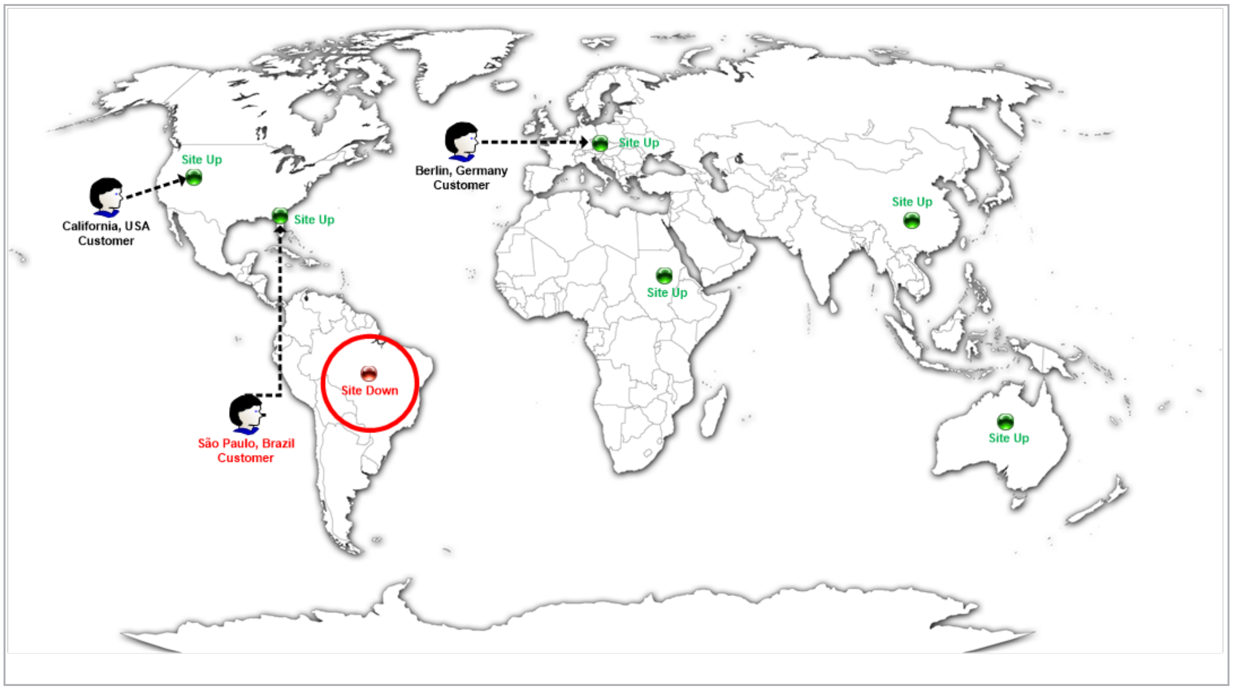
Partners are two or more GEO units in an active-active mode.

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.

2.3 Fail Over



Fail Over allows 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 will be answered by the nearest (by proximity) target. If this is not possible, the target with the lowest requests will be picked. For example, if a request from Ireland is received, but the site assigned to **Ireland** is unavailable, a site assigned to **Europe** will be selected. If the site assigned to Europe is also unavailable, a site assigned to **Everywhere** will be selected. If this too is unavailable, the least requested of the available sites will be selected. 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.

2.4 Failure Delay and Site Recovery Mode

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 fail-over. However, if needed it is possible to set a **Failure Delay**. **Failure Delay** is very important in Exchange data centers.

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 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 has been detected. If, after the delay, the site has recovered, the failover is not initiated. If the site has not recovered, the failover is initiated as per normal.

If a **Failure Delay** has been set, another option becomes available underneath it – **Site Recovery Mode**. Two modes are available:

- **Automatic:** The site is brought back into operation immediately upon site recovery
- **Manual:** Once the site has failed, disable the site. Manual intervention is required to restore normal operation.

2.5 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 will be 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.

So, 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 will be 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.

2.6 Public Requests & Private Requests

The **Public Requests & Private Requests** options replace the old **Isolate Public/Private Sites** option which was available on LoadMasters with firmware up to 7.1-29. The new settings offer administrators greater flexibility when configuring an FQDN.

These new settings allow administrators to 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.

The following table outlines settings and their configurable values:

Setting	Value	Client Type	Site Types Allowed
PublicRequests	Public Only	Public	Public
	Prefer Public	Public	Public, Private if no public
	Prefer Private	Public	Private, Public if no private
	Any 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

Setting	Value	Client Type	Site Types Allowed
	Any Sites	Private	Private and Public

2.7 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.

2.8 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

2.9 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.

2.10 Selection Criteria

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.

2.10.1 Round Robin

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

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.

2.10.2 Weighted Round Robin

This method expands on the functionality of simple round robin by allowing incoming requests to be distributed across the cluster in a sequential manner, while also taking account of a static pre-assigned “weighting” of IP address end-points.

The administrator simply defines the capacities of the IP address end-points available by weighting the IP address end-points. The most efficient Data Center A, for example, is given the weighting 100, whilst a much less powerful Data Center B is weighted at 50. This means that Data Center A would always receive two consecutive requests before Data Center B receives its first one, and so on.

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

2.10.3 Fixed Weight

The highest weight IP address end-point is only used when other IP address end-point(s) are given lower weight values. However, if highest weight server falls, the IP address end-point with the next highest weighted number will be available to serve clients. The weight for each IP address end-point should be assigned based on the priority among IP address end-point(s). When the failed IP address end-point becomes available, it automatically starts receiving requests.

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

2.10.4 Real Server Load

Requires integration with LoadMaster, this allows you to obtain datacenter-level metrics from LoadMaster which are used in real-time to direct clients to the cluster that’s least busy. The GEO LoadMaster will poll the connection statistics of LoadMaster and use a portion or all of the available data to determine overall level of busyness for the relevant Virtual Service. The cluster with the lowest value receives the requests. Each IP address end-points must be attached to a Cluster and the Checker option must be **Cluster Checks**.

The LoadMaster that is being polled needs to have an Adaptive Agent setup in order to determine the cluster’s level of busyness. For further information on the Adaptive Agent, please refer to the **Install Adaptive Agent – Windows, Technical Note**.

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

2.10.5 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 in order to ensure correct balancing.

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.

In order 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 will be rejected.

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

2.10.6 Location Based

The client source IP address is geocoded in real-time for its defined location. As an example, using country or continent you can selectivity assign each region to a specific IP address end-point and ensure that client requests that have a matching location definition are directed to the corresponding data center.

Country specificity overrides continent specificity when assigned to the same IP address end-point. If a target is configured for a country and a different target is configured for a continent containing that country, the target with the country will be selected only if the request originates from that country. So, the target with the highest depth in the hierarchy wins. The hierarchy is:

Everywhere > Continent > Country

Client location is matched against the ordered list of IP address end-points, visible IP address end-point order in the Web User Interface is relevant to match criteria. If there is more than one site with the same country code, requests will be distributed in a round robin fashion to each of the sites.

This selection criterion is dependent on the geographical IP database.

2.10.7 All Available

The **All Available** selection criteria returns all possible healthy targets for an A, AAAA or ANY query request. 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.

2.10.8 IP Range Selection Criteria

In the **IP Range Selection Criteria** menu option, you can specify a 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 internal 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**.

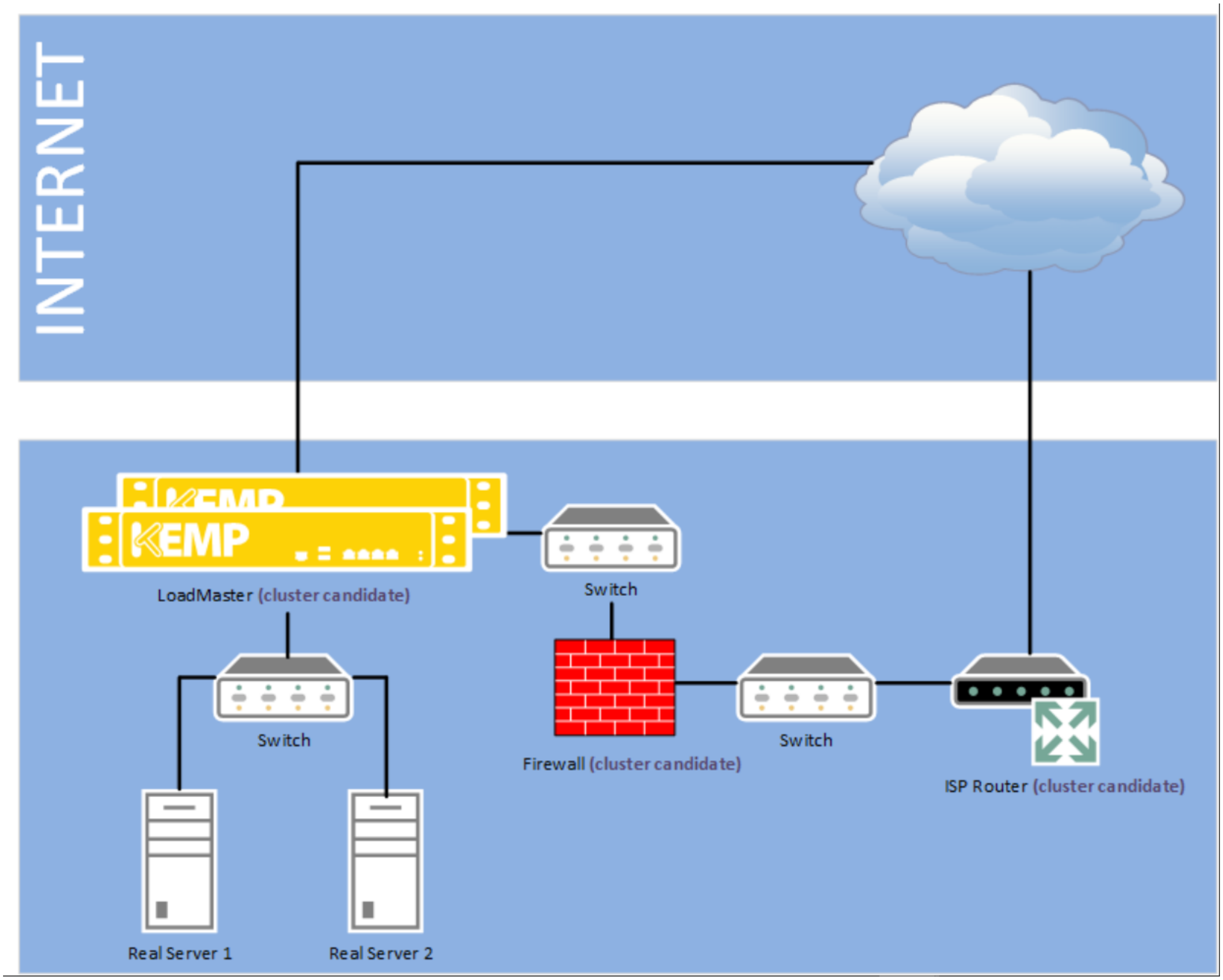
GEO supports subnet precedence for custom-defined IP address ranges in **IP Range Selection Criteria**. For example:

- 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.

2.11 Clusters

A cluster is a logical grouping of devices, which can be physically defined as any IP address that can be checked for availability. Clusters allow for a consolidated health check and also allow for a grouping of Real Servers, LoadMasters or other resources defined in FQDNs, allowing for site or data center-level management of devices. 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.


INTERNET
KEMP
LoadMaster (cluster candidate)
Switch
Switch
Firewall (cluster candidate)
Switch
ISP Router (cluster candidate)
Real Server 1
Real Server 2

- **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

2.11.1 Cluster Types

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

- **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.

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 via SSH).

2.12 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

Layer	Type	Description
		(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 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 in order for health checks to function correctly. If the **Checker** type is set to **Cluster Checks** and the cluster **Type** (in **Global Balancing > Manage**

Layer	Type	Description
		Clusters > Modify > Type) is set to **Remote LM**, you must also select the associated Virtual Service from the **Mapping Menu** drop-down list. 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 will displays a list of Virtual Service IP addresses from that LoadMaster. It lists each Virtual Service IP address with no port, as well as all of the Virtual IP address and port combinations. Please select the Virtual IP address that is associated with this mapping. If a Virtual Service with no port is selected, the health check will check all Virtual Services with the same IP address as the one selected. If one of them is in an “Up” status, the FQDN will show as “Up”. The port does not come in to consideration. If a Virtual Service with a port is selected, the health check will only check against the health of that specific Virtual Service when updating the health of the FQDN.

2.13 IP Blacklist

It is possible to download blacklist rules from KEMP in order to block access from IP addresses which are on the blacklist. A whitelist can be manually specified which will override the blacklist.

For further information on this feature, including instructions on how to configure the IP Blacklist Settings, please refer to the **GEO, Feature Description**.

2.14 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.

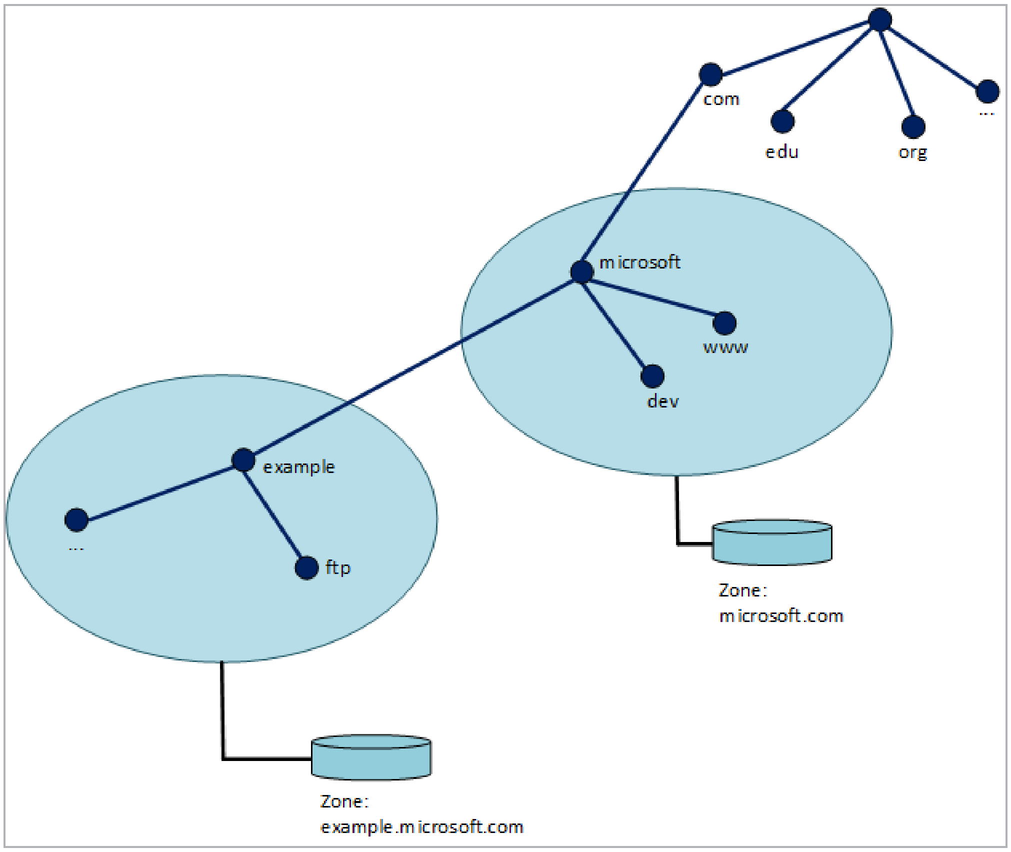
DNSSEC adds four new resource record types, which are:

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

These 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. 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 find out how to configure DNSSEC in the LoadMaster, refer to the **GEO Feature Description** on the KEMP Documentation Page.

2.15 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.

2.16 Specify what Interfaces to use for GEO Responses and Requests

By default, only the default gateway interface is used to listen for and respond to DNS requests.

There is a field called **Use for GEO Responses and Requests** which 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. To get to this option, go to **System Configuration > Network Setup** and select the relevant interface number.

This option cannot be disabled for the interface which has the default gateway. By default, this is eth0.

2.17 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.

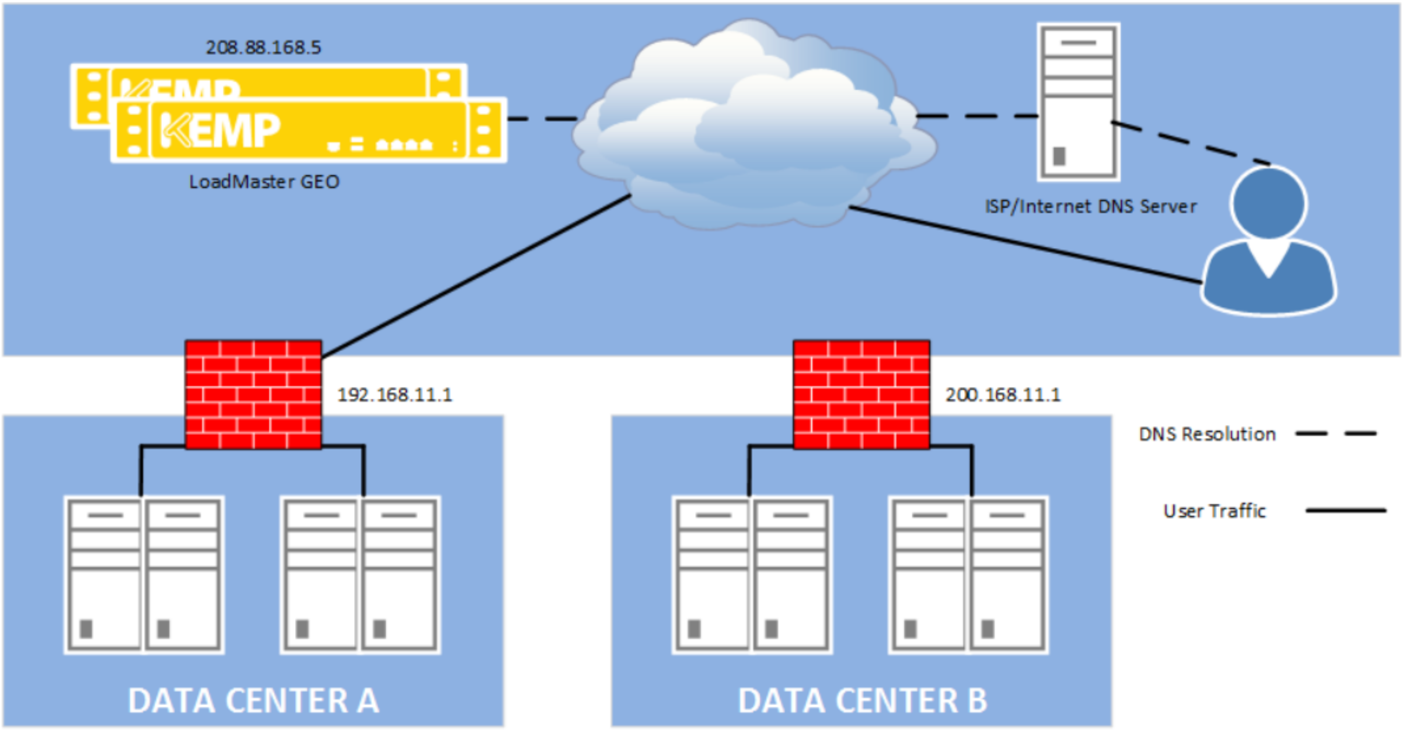
Enabling this option adds another option to the **Interfaces** screen – **Use for Default Gateway**.

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

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

2.18 GEO Example

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



1. A client enters a website address, for example **www.web.example.com**, into the address bar of their web browser.

2. The resolution request is passed to the Authoritative DNS Server for the domain.

3. Usually the Authoritative DNS Server would resolve the request but in this case the authority has been delegated to the LoadMaster.

4. The Authoritative DNS Server has an A record pointing to the LoadMaster and a corresponding PTR record for the reverse lookup by IP.

5. For each hostname that has been delegated to the LoadMaster, an NS record will have been created and set to the A record created for the LoadMaster, for example:

Record Types (A and PTR)

lm1.example.com = 208.88.168.5

Record Type (NS)

www.example.com = lm1.example.com

6. The Authoritative DNS Server passes the resolution request to the LoadMaster.

7. The LoadMaster looks up the list of configured FQDNs to decide what IPs the FQDN resolves to. In this case, the FQDN resolves to either Data Center A (192.168.11.1) or Data Center B (200.168.11.1).

8. The LoadMaster knows if both of the Data Centers are healthy or not as it is performing regular health checks.

9. The LoadMaster decides which IP address to resolve the request to, based on the Selection Criteria.
In this case, we assume that the request is resolved to Data Center A (192.168.11.1).

10. If, for some reason, Data Center A failed the health check, the request would have resolved to Data Center B.

11. The LoadMaster passes the IP address back to the DNS Server which passes it back to the client.

12. The client connects directly to Data Center A (192.168.11.1).

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation:

Web User Interface (WUI), Configuration Guide

Install Adaptive Agent – Windows, Technical Note

GEO, Feature Description

Document History

Date	Change	Reason for Change	Version	Resp.
Oct 2014	Release updates	Updates for 7.1-22/2.1-22	1.10	LB
Jan 2015	Release updates	Updates for 7.1-24/2.1-24	1.11	LB
Jan 2015	Minor changes	Defects resolved	1.12	LB
Sep 2015	Release Updates	Updates for 7.1-30	3.0	KG
Oct 2015	Minor changes	Updated header and footer	4.0	LB
Jan 2016	Minor changes	Updated Copyright Notices	5.0	LB
Mar 2016	Release updates	Updates for 7.1-34	6.0	LB
July 2016	Release updates	Updates for 7.1.35	7.0	LB
Jan 2017	Release updates	Updates for 7.2.37	8.0	LB
July 2017	Minor change	Enhancement	9.0	POC