



LoadMaster DR

Configuration Guide

Release 1.0-55

Updated: July 2011

World Headquarters

KEMP Technologies Inc.
12 Old Dock Road
Yaphank, NY 11980
U.S.A.

+1 631.345.5292

EMEA Headquarters

KEMP Technologies Ltd.
Mary Rosse Centre
Holland Road, National Tech. Park
Limerick, Ireland

+353 (61) 260 101

www.kemptechnologies.com

Disclaimer

© 2002-2011 KEMP Technologies, Inc. All rights reserved. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc..

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster product line including software and documentation. The use of the LoadMaster Exchange appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows is a registered trademarks of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Table of Contents

LoadMaster DR Overview	4
High Availability (HA).....	4
Speed.....	4
Scalability.....	4
Manageability	5
Concepts	5
Deployment	6
DNS Responder	6
High Availability (HA).....	6
Remote Administration	7
DNS Responder System Configuration	7
Source of Authority (SOA)	8
Resources Check Parameter	8
Cluster.....	8
Overview.....	8
Full Qualified Domain Name (FQDN).....	9
Real Server/Cluster Health Checking.....	9
Load Balancing Algorithms/Selection Criterion	10
Round Robin	10
Weighted Round Robin	10
Fixed Weighted	10
Real Server Load	10
DNS Integration/Delegation.....	11
Web User Interface	11
Home	11
Global Balancing.....	12
Manage FQDNs.....	12
Manage Clusters	13
Miscellaneous Parameters	14
Statistics.....	14
System Configuration	15
Interfaces.....	15
Local DNS Configuration.....	15
Route Management.....	16
Access Control	16
System Administration.....	17
Logging Options	19
Miscellaneous Options.....	23
HA Parameters.....	24
Glossary	28
Index.....	30
Document History	31

LoadMaster DR Overview

LoadMaster DR (LM-DR) offers the ability to move beyond the single datacenter, allowing for high availability in a multi datacenter environment. When a primary site is down, traffic is diverted to the Disaster Recovery site. Also included in LoadMaster DR is the ability to ensure clients connect to their fastest performing datacenter.

The LM-DR offers the same management interfaces as KEMP's LoadMaster product suite, including all the foundation technology such as syslog logging, email notifications, interface bonding, and Gigabit support. LoadMaster DR provides advanced application health checking, to ensure that unavailable services or datacenters are not visible to clients. Health checking can occur at the services level or even the site level, allowing for flexible decision making about when traffic should be diverted per Fully Qualified Domain Name (FQDN).

LoadMaster DR offers "Round Robin" load balancing for all active datacenters, which includes support for weights and a chained failover option for disaster recovery. LoadMaster DR securely and seamlessly integrates with LoadMaster to offer "Real Server Load" load balancing, in which LoadMaster DR uses local datacenter metrics provided by LoadMaster, allowing clients to connect to the least busy datacenter.

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

High Availability (HA)

LoadMaster DR helps prevent service outages by quickly detecting server and datacenter failures and then directing traffic. Monitoring and load balancing are based on layers 3 and 4 of the Open Systems Interconnection Basic Reference Model (OSI). Included in HA is the ability to have two appliances, protecting against introduction of a single point of hardware/network connectivity failure. Each individual LoadMaster DR can also be configured to provide network link-layer redundancy.

Speed

LM-DR's intelligence ensures that your mission critical servers are continuously available and performing reliably. LoadMaster DR 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, LoadMaster DR eliminates server overload conditions and round trip propagation delays that may slow performance, allowing you to increasing end user application speed.

Scalability

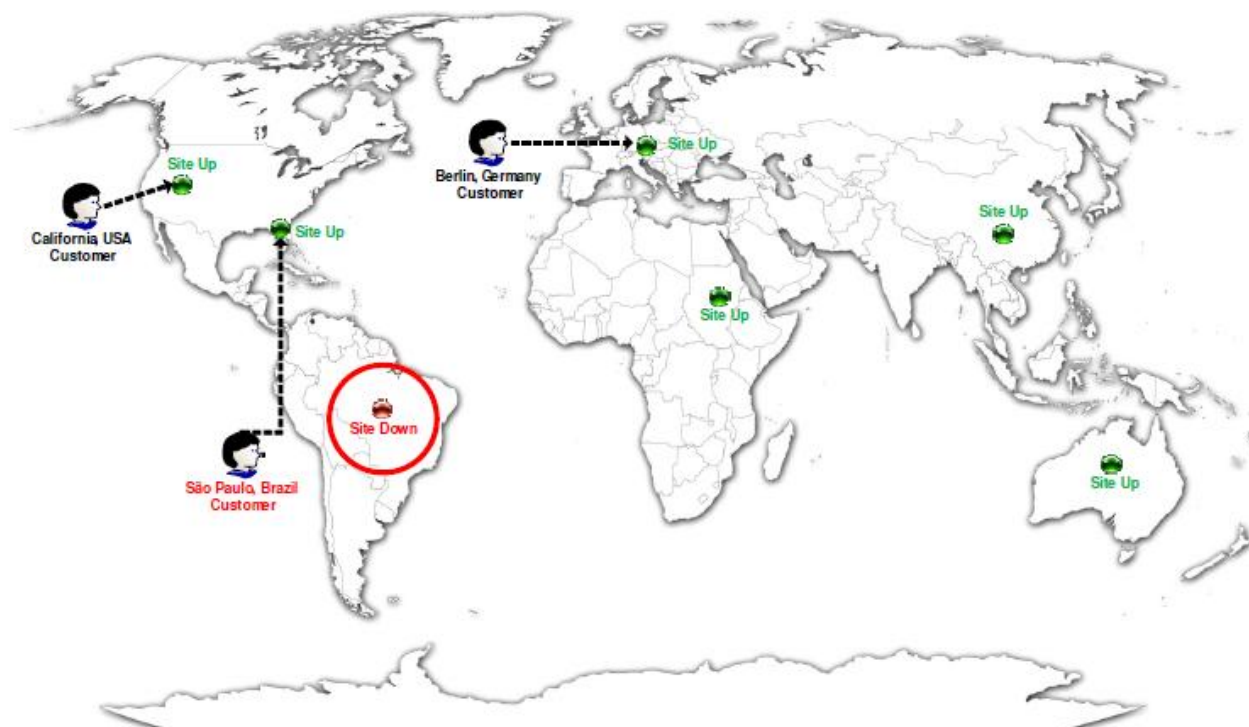
LM-DR solves the scalability dilemma in the common adage "Growth is the challenge, scalability is the key". LM-DR solves the scalability dilemma by continuing to support increasing network server workloads and still providing high reliability. LoadMaster offers:

- 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 and enables many inexpensive servers to function as a single, virtual server.
- Reduces the single point of failure and expense inherent with a single large server, and allows for the orderly addition of new servers, or the routine maintenance or upgrades of servers 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

LM-DR is easy to set up, and easy to manage. LoadMaster DR is a self contained 'plug and play' appliance that doesn't require the additional installation of software on your servers. Network management is made easy, administrators can deploy new servers and take individual servers offline for routine maintenance without disrupting services to end users. Integrating LM-DR into an existing DNS infrastructure can be done with no service impact and allows for distributed administration.

E.g. Multi Datacenter Load Balancing example



Concepts

- Cluster = A device responsible for allowing connectivity to more than one device. E.g. Edge router, firewall, or load balancer.
- FQDN = Fully Qualified Domain Name
- Real Server (RS) = Target host IP, generally a server or appliance.
- LM = LoadMaster, the application delivery controller (server load balancer).
- LM-DR = LoadMaster DR
- One Armed = Only one Ethernet interface is used for inbound and outbound traffic. (Used interchangeably with Flat-based.)
- Access Code = An Access Code will be generated during the initial setup of the LoadMaster. You must contact your KEMP Technologies representative for your 60day evaluation or your full purchased license key.
- Network Side = Interface eth0
- Two armed = Multi armed, configuring more than one logic subnet, generally using physical ports, but includes using VLANs, and addition subnets.
- ISP = Internet Service Provider
- Virtual Service (VS) = Virtual Internet Protocol Addressed used to load balance to Real Servers on

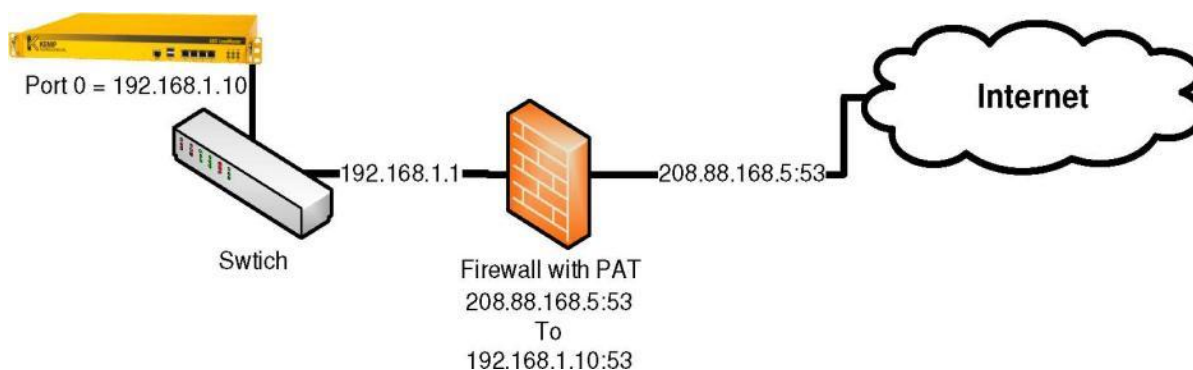
- LoadMaster. NAT = Network Address Translation
- NAT Overload = Same as Port Address Translation (PAT)
- WUI = Web User Interface

Deployment

DNS Responder

Before setting up the LoadMaster DR, take a moment to consider how the LoadMaster DR will fit into your network. LoadMaster DR has been designed for a one armed topology, either behind a firewall which is forwarding (PAT/NAT Overload) DNS traffic to the eth0 (Port 0) of LoadMaster DR or at the network edge with no firewall. There is no technical restriction to placing LoadMaster DR before or parallel to a firewall and assigning a Public IP to Port 0.

In a one armed configuration, the DNS responder service can be configured for ANY subnet. The LoadMaster DR connects to a Layer 2 network through a single interface, eth0. (Throughout this documentation the terms eth0, Port 0 and “Network side” may be used interchangeably.)

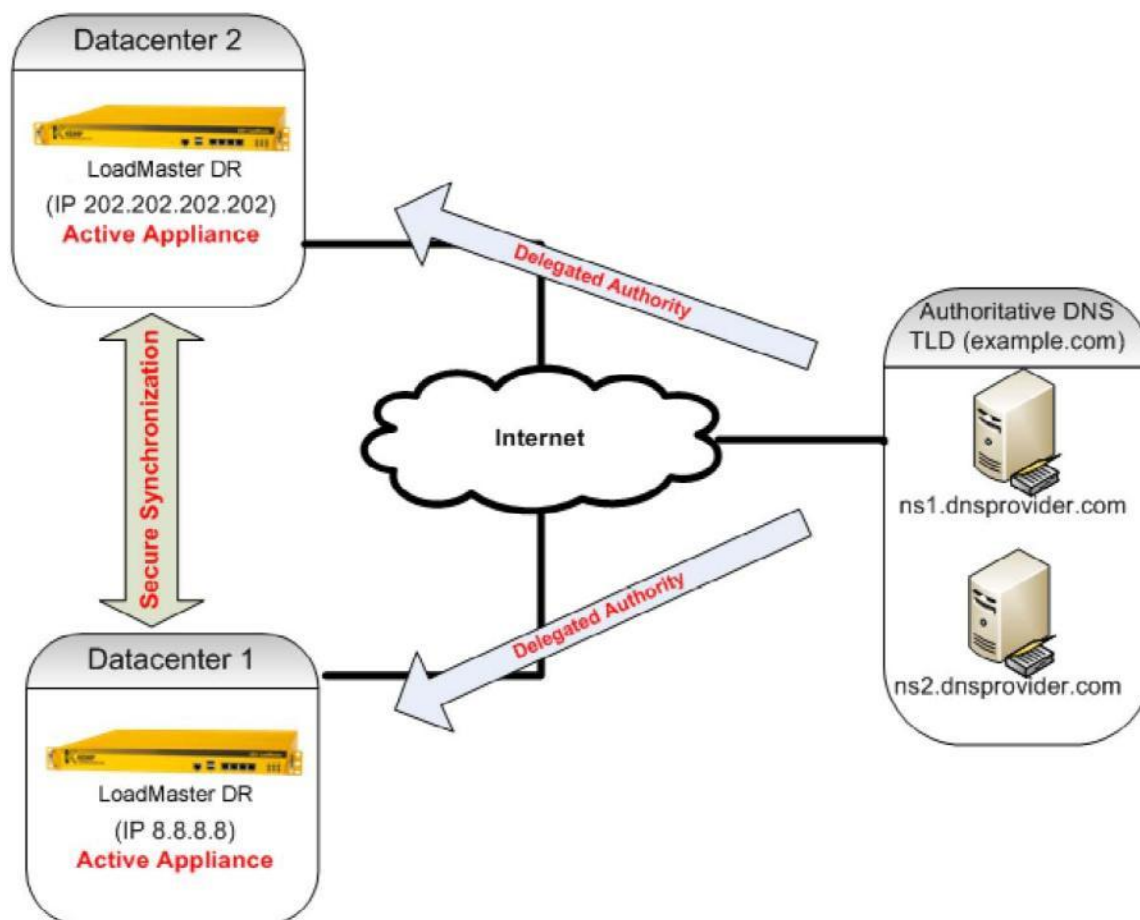


If you already have a firewall in place performing PAT to a DMZ in a non-routable (RFC1918) IP space (e.g.,

192.168.x.x or 10.x.x.x), please make sure a 1to1 PAT for port 53 UDP/TCP exists to the LoadMaster DR. We **do not recommend** a Layer 3 source IP NAT to the LoadMaster DR as it will mask source IP visibility during geographical coding operations, all devices before LoadMaster DR should be transparent. The LoadMaster DR(s) can be located on the DMZ with no large scale network changes required. *As depicted above*, the default gateway of LoadMaster should point to the firewall.

High Availability (HA)

LoadMaster DR has support for a Active/Active deployment where each LoadMaster DR is synchronizing information in a close to real-time manner over a SSH. When deploying more than a single LoadMaster DR we recommend placing each LoadMaster DR at different datacenters. Management of the HA pairs can be done via either appliance; changes synchronize in the background.



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. LoadMaster DR supports multi-arm configurations where the administrative access has been moved off the default eth0 port. The recommended interface for remote administration is HTTPS.

When negotiating a HTTPS connection with LoadMaster DR 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 DR 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 left navigation.

DNS Responder System Configuration

Configuration of global parameters controls the behavior of the entire LoadMaster DR. The Source of Authority information is not required for basic functionality; however this metadata should be populated to accurately represent the LoadMaster DR DNS server. Resource Check Parameters define the global health checking that occurs from LoadMaster DR to Clusters and Real Servers.

These options can be found in the WUI under

- ▶ **Global Balancing**
- ▶ **Miscellaneous Params**
- ▶

Source of Authority (SOA)

Source of Authority is defined in [RFC 1035]. The SOA defines global parameters for the zone (domain). There is only one SOA record allowed in a zone file.

Name Server is defined as the forward DNS entry configured in the Top Level DNS. written as a Fully qualified Domain Name (FQDN and ends with a dot), for example, geo1.examplecom

The SOA Email is to publish a mail address of a person or role account dealing with this zone with the "@" converted to a ".". The best practice is to define (and maintain) a dedicated mail alias "hostmaster" [RFC 2142] for DNS operations.

TTL is the Time to Live value which dictates how long the reply from LoadMaster DR can be cached by other DNS servers or client devices. This value should be as practically low as possible. The time interval is defined in minutes.

Resources Check Parameter

Check Interval is defined in seconds and is the delay between health checks, this includes clusters and FQDNs.

Connection Timeout is defined in seconds. The timeout is the allowed maximum wait time for a reply to a health check.

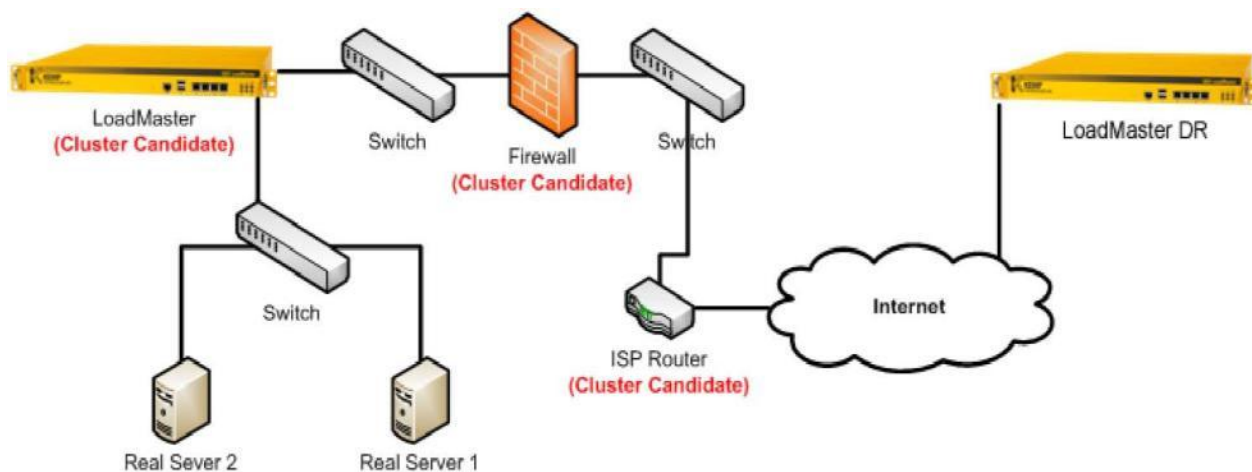
Retry attempts is the number of consecutive times in which a health check must fail before it is marked down and removed from the load balancing pool.

The maximum detection window for failed clusters or FQDNs is the (Check Interval + Connection Timeout) multiplied by Retry attempts.

Cluster

Overview

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 checking and also allow for a grouping of Real Servers defined in FQDNs, allowing for site or datacenter 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.



For assuring data center visibility, checking the ISP's edge router will quickly allow you to detect when your ISP's network connectivity is lost.

Checking the firewall will confirm the ISP network is available and provides visibility to the first arm of equipment located at your data center.

Checking a load balancer (LoadMaster) will allow you to confirm your ISP is available, your network infrastructure is available and that your Real Servers are responding as expected.

Full Qualified Domain Name (FQDN)

A Full Qualified Domain Name 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 subdomain. Each FQDN is considered an A record.

Each distinct hostname must be configured in LoadMaster DR individually. A LoadMaster DR does not support wildcard DNS entries, such as `*.kemptechnologies.com`

Example FQDN's include hostnames like `www.kemptechnologies.com` and `www.kemptechnologies.co.uk`

LoadMaster DR support comingling of top level domains, you can create a FQDN for `www.example.com` and also `www.kemptechnologies.com` Domainless hostnames are also supported, such as "mail"

Real Server/Cluster Health Checking

The LM-DR Load Balancer utilizes Layer 3, Layer4 and Layer7 health checks to monitor the availability of the Real Servers and Clusters. In case that one of the servers does not respond to a health check within a 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 it can be determined that this real server is back online.

Health checks originate from LoadMaster DR; it is therefore important to make sure LoadMaster DR has access to each Cluster and Real Server IP. If you notice that all checks fail, double check your default gateway and ensure the gateway is operating correctly.

Layer	Type	Description
None	None	No check occurs.
Layer 3	ICMP	The LoadMaster sends ICMP echo requests (pings) to the Real Servers. A Real Server fails this check when it doesn't respond with an ICMP echo response in the configured response time for the configured number of retries.
Layer 4	TCP	The LM-DR attempts to open TCP connection to the Real Server on the configured service port: It sends a TCP SYN packet to the server on the 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. The port can be configured.
Layer 7	Remote LM	A SSH connection is attempted; native LoadMaster statistics are obtained and matched against the FQDN Real Server. If no matching Virtual Service IP is found the list of Real Servers cluster is marked as down. Permission to connect must be granted on LoadMaster

Load Balancing Algorithms/Selection Criterion

This 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 criteria.

Round Robin

With this method incoming requests are distributed sequentially across the Real Servers, i.e. the available servers.

If this method is selected, all the Real Servers assigned to a FQDN should have similar resource capacity and host identical applications. Choose round robin if all servers have the same or similar performance and are running the same load. Subject to this precondition, the round robin system is a simple and effective method of distribution.

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

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

Weighted Round Robin

This method mitigates a weakness of 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 Real Server.

The administrator simply defines the capacities of the servers available by weighting the Real Server. 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

The highest weight Real Server is only used when other Real Server(s) are given lower weight values. However, if highest weight server falls, the Real Server with the next highest priority number will be

If Real Servers have the same weight, Round Robin load balancing is preformed over these Real Servers

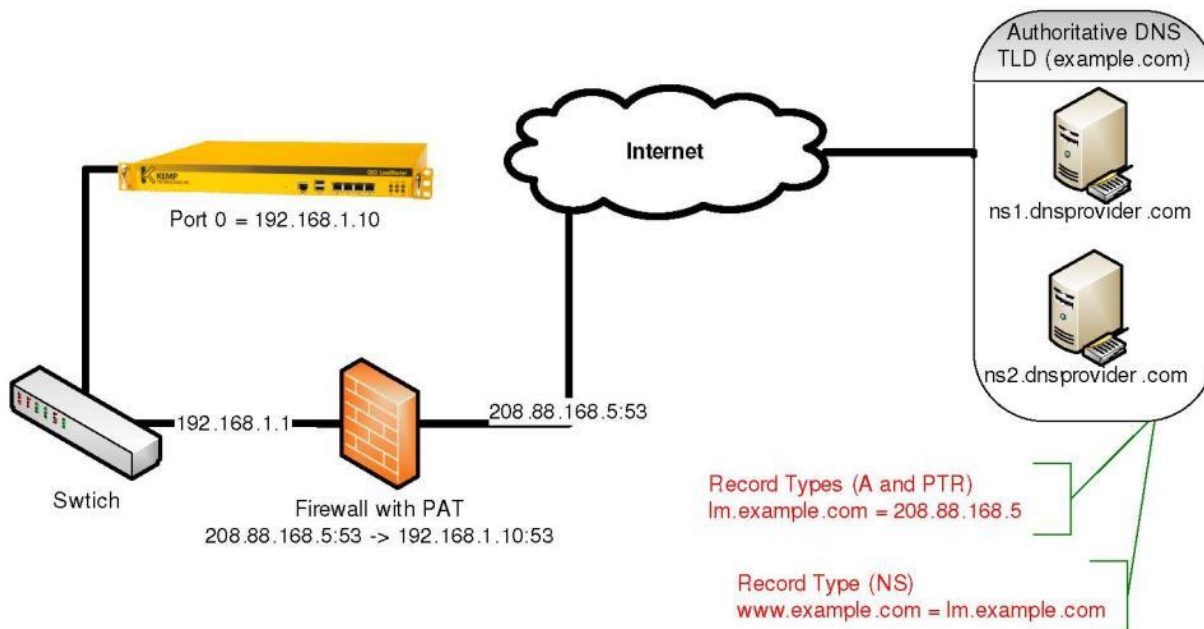
This selection criterion is not dependent on the geographical IP database.

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. LoadMaster DR will poll the connection statistics of LoadMaster and use a portion or all of the available data to determine overall level of busyness. The cluster with the lowest value receives the requests. Each Real Server must be attached to a Cluster and the Checker must be “Cluster Checks”.

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

DNS Integration/Delegation



Integrating LoadMaster DR with your Authoritative DNS can be completed with only a few new DNS records.

1. Create a new A record pointed to LoadMaster DR. (e.g. lm.example.com) and the corresponding PTR record for the reverse lookup by IP. Forward confirmed reverse DNS support is required.
2. For EACH hostname you need delegated to LoadMaster DR create a NS record and set the value to the A record created for LoadMaster DR in the previous step. (e.g. www.example.com to lm.example.com)
3. Optional High Availability configuration: Repeat Step 1) for the second LoadMaster DR using a unique hostname lm2.example.com Repeat Step 2) using the second LoadMaster DR resulting in two NS records for www.example.com one pointing to lm1.example.com and one to lm2.example.com

Web User Interface

Home

This section corresponds directly with the Web User Interface and the menu navigation.

An introduction page showing the vital information of the LoadMaster.

IP address	192.168.201.128
Machine Identifier	sqNE4TT8Fq99
Boot Time	Wed Jul 20 16:19:30 UTC 2011
LoadMaster DR Version	1.0-71
License	Activation date: July 20 2011 Licensed until: Unlimited
CPU Load	1%
TPS	Total 0 (SSL 0)
NetLoad	Mbits/sec
eth0	0.0

The CPU load and Net load data are updated every 5 seconds.

Global Balancing

Manage FQDNs

FQDN's (Fully Qualified Domain Names) may be added, modified or deleted.

To add:

1. Type in the domain name and click **Add FQDN**.
2. The next screen displayed is the Modify FQDN screen. Input the selection criteria, the IP address of the domain and, if needed, the cluster where the IP address is located, and click **Add Address**.
3. At this point you have configured the FQDN. You can add another IP address to the domain, change the type of checking to be performed on the current IP address, or click **<Back** to view the list of configured FQDN's.

Configure kemptechnologies.com.

Selection Criteria Round Robin

IPaddress	Cluster	Checker	Availability	Parameters	Operation
<input type="text"/>	Select Cluster				<input type="button" value="Add Address"/>
10.200.0.67	Test	Icmp Ping Addr <input type="text"/>	Up		<input type="button" value="Disable"/> <input type="button" value="Delete"/>
10.200.0.68	Select Cluster	Tcp Connect Addr <input type="text"/> : 80	Up		<input type="button" value="Disable"/> <input type="button" value="Delete"/>

To Modify:

1. Click the **Modify** button of the desired FQDN..
2. Change the desired parameters and click the **<Back** button.
3. Selection criteria are chosen from a drop-down list:

Round Robin - traffic distributed sequentially across the server farm (cluster), i.e. the available servers.

Weighted 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.

Fixed Weighting - the highest weight Real Server is used only when other Real Server(s) are given lower weight values.

Real Server Load - LoadMaster contains logic which checks the state of the servers at regular intervals and independently of the configured weighting.

Round Robin

- Round Robin
- Weighted Round Robin
- Fixed Weighting
- Real Server Load

Configured Fully Qualified Names

Fully Qualified Domain Name	Type	IPaddress	Cluster	Checker	Availability	Requests/s	Parameters
<input type="button" value="Modify"/> kemptechnologies.com.	Round Robin	10.200.0.67	Test	ICMP Ping	Up	0	
		10.200.0.68		TCP Connect (80)	Up	0	

To Delete IP Address:

1. Click the **Modify** button of the desired FQDN..
2. Click the **Delete** button of the IP address to delete and click the **<Back** button.

To Delete the FQDN:

1. Click the **Modify** button.

- Click the **Delete <domain name>** button and click the **<Back** button.



CAUTION –once deleted there is no UNDO feature. Use DELETE with care.

Manage Clusters

Clusters, a group of LoadMaster-DR's working in conjunction, may be added, modified or deleted as follows:

Configured Clusters						
IPaddress	Name	Location	Type	Checker	Availability	Operation
96.56.160.205	test	40°37'12"N 73°59'12"W	Default	None	Up	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
96.56.160.204	test2	40°37'12"N 73°59'12"W	Default	None	Up	<input type="button" value="Modify"/> <input type="button" value="Delete"/>

To Add:

- Click the **Add Cluster** button.
- Input the IP address and the desired name of the cluster and click the Add Cluster button.

Add a Cluster	
IP address	<input type="text" value="96.56.160.207"/>
Name	<input type="text" value="Test3"/>
<input type="button" value="Cancel"/> <input type="button" value="Add Cluster"/>	

To Modify:

- Click the **Modify** button of the desired cluster.
- Change the desired parameters and click the **<Back** button. **Type** may be default (DR operation) or Remote LM and Checkers may be Icmp Ping or Tcp Connect. If desired, input the Latitude and Longitude of the location of the LoadMaster-DR.

Modify Cluster test					
<input type="button" value="<-Back"/>					
IPaddress	Name	Location	Type	Checkers	Operation
96.56.160.205	<input type="text" value="test"/> <input type="button" value="Set Name"/>	Location: 40°37'12"N 73°59'12"W <input type="button" value="Show Locations"/>	Default	None	<input type="button" value="Disable"/>
Manually set location: 0°0'0"N 0°0'0"W Resolved location: 40°37'12"N 73°59'12"W <input type="text" value="0"/> : <input type="text" value="0"/> : <input type="text" value="0"/> N <input type="text" value="0"/> : <input type="text" value="0"/> : <input type="text" value="0"/> W <input type="button" value="Set Location"/>					

To Delete the Cluster:

- Click the **Delete** button.



CAUTION –once deleted there is no UNDO feature. Use DELETE with care.

Miscellaneous Parameters

Source of Authority

Source of Authority	<input type="text"/>	Set SOA
Name Server	<input type="text"/>	Set Nameserver
SOA Email	<input type="text"/>	Set SOA Email
TTL	1	Set TTL value

Resource Check Parameters

Check Interval	30	Set Check Interval
Connection Timeout	15	Set Timeout value
Retry attempts	2	Set Retry Attempts

Source of Authority

Set the response sent for Source of Authority requests.

Name Server

Set the response sent for Name Server requests.

SOA Email

Set the response Email string for SOA requests.

TTL

Set the Time To Live of the responses returned by the LoadMaster DR.

Check Interval

Set how often devices will be checked.

Connection Timeout

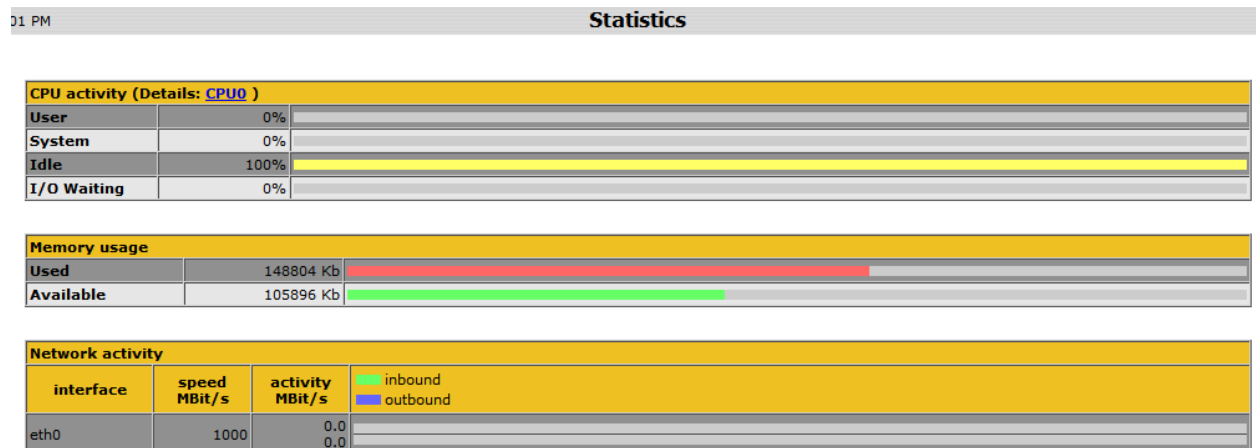
Set the timeout of the check request.

Retry Attempts

Set the number of times the check will be retried before the device is marked as Failed.

Statistics

Shows the activity for the Loadmaster DR.



CPU

This table displays the following CPU utilization information for a given Balancer:

Use	the percentage of the CPU, which is spent in processing in user mode
System	the percentage of the CPU spent processing in system mode
I/O Waiting	the percentage of the CPU spent waiting for I/O to complete
Idle	the percentage of CPU, which is idle



The sum of these 4 percentages will = 100%

Core Temp temperature for each CPU core is displayed for LoadMaster DR hardware appliances by clicking the link for each CPU. Temperature will not show on a Virtual LoadMaster DR statistics screen.

Memory

This bar graph shows the amount of memory in use and the amount of memory free on the unit.

Network Activity

These bar graphs show the current network throughput on each interface.

System Configuration

This section provides access to the parameters of the LoadMaster and the systems as an entire entity and is shown on the left side of the screen.

Interfaces

Describes the external network and Internal network interfaces. The screen has the same information for the eth0 and eth1 Ethernet ports. The example below is for eth0 on a non HA unit. Also see VLAN bonding in Section O. If you have older infrastructure that does not support VLAN tagging, you may associate additional subnets to any interface by designating a base network address and a subnet mask. The LoadMaster will not create any routes to these additional subnets. If needed, an external device supporting router-on-a-stick configuration can be deployed alongside the LoadMaster.

Network Interface 0

Interface Address (xx.xx.xx.xx[/ss])	<input type="text" value="10.200.0.65/8"/>	<input type="button" value="Set Address"/>
Link Status	Speed: 1000Mb/s, Full Duplex	
	Automatic	<input type="button" value="Force Link"/>

Subnets on this Interface

Subnet	Local Address	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Local DNS Configuration

Set Hostname

Current Hostname	<input type="text" value="VLMDR"/>	<input type="button" value="Set Hostname"/>
------------------	------------------------------------	---

The Hostname is Used for Diagnostic logging

DNS Servers	
DNS NameServer (IP Address)	Action
<input type="text"/>	<input type="button" value="Add"/>
10.0.0.1	<input type="button" value="Delete"/>

DNS Search Domains	
DNS Search Domains	Action
<input type="text"/>	<input type="button" value="Add"/>
kemptechnologies.com	<input type="button" value="Delete"/>

The maximum configuration is 3 DNS' and 6 search domains.

Route Management

This option permits the configuration of default and static routes. The Load Master requires a **default gateway** through which it can communicate with the Internet.

The default gateway must be on the 10.0.0.0/8 network	
Default Gateway Address	<input type="text" value="10.0.0.1"/> <input type="button" value="Set Default Gateway"/>

Further routes can be added. These routes are static and the gateways must be on the same network as the Load Master. To segment traffic you can also leverage the Virtual Service level default gateway.

Destination	Gateway	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Access Control

Packet Filter Enabled

Using this toggle option the Packet filter can be activated/deactivated. If the filter is not activated, the Load Master acts as a simple IP-forwarder. When the filter is activated, only the Virtual Service addresses can be addressed.

Packet Filter	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Rejection method	Drop <input checked="" type="radio"/> Reject <input type="radio"/>

Reject/Drop blocked packets

When a connection request is received from a host, which is blocked using the ACL, the request is normally ignored (dropped). The Load Master may however be configured to send back an ICMP reject packet. For security reasons it is usually best to drop any blocked requests.

Access control Lists

The Load Master supports a "blacklist" Access Control List system. Any host or network entered into the Access Control List will be blocked from accessing any service provided by the Load Master.

Blacklist	
Blocked addresses	Operation
<input type="text"/>	<input type="button" value="Block Address(es)"/>

Whitelist	
Allowed addresses	Operation
<input type="text"/>	<input type="button" value="Allow Address(es)"/>

The Access Control List is only enabled when the Packet Filter is enabled. The whitelist allows a specific IP address or address range access. If the address or range is part of a larger range in the blacklist, the whitelist will take precedence for the specified addresses.

This option allows a user to add or delete a host or network IP address to the Access Control List. Only “dotted-quad” IP addresses are allowed. Using a network specifier specifies a network.

I.e. Specifying 192.168.200.0/24 will block all hosts on the 192.168.200 network.

System Administration

These options control the base level operation of LoadMaster. It is important to know that applying changes to these parameters in a HA pair must be done using the floating management IP. Many of these options will require a system reboot. When configuring these parameters only the active system in a pair is affected.

User Management

Change the appliance password. This is a local change only and does not affect the password of the partner appliance in a HA deployment.

Change Password	
Current Password	<input type="text"/>
New Password	<input type="text"/>
Re-enter New Password	<input type="text"/>
<input type="button" value="Reset"/> <input type="button" value="Set Password"/>	

Other Users	
User	<input type="text"/>
Password	<input type="text"/>
Use RADIUS Server	<input type="checkbox"/>
<input type="button" value="Add User"/>	

No Other Users

The User Management screen allows you to change a current Users password, add a new User and associated password or change the permissions for an existing User (see below).

Permissions for User CJMtest	
System Backup	<input type="checkbox"/>
All Permissions	<input type="checkbox"/>
Geo Control	<input type="checkbox"/>
Allowed Network 1	None Assigned ▾
Allowed Network 2	None Assigned ▾
<input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="SetPermissions"/>	

In this screen you may set the level of User permissions insofar as what configuration changes the User is allowed to perform. The primary User, bal, always has full permissions. Secondary Users may be restricted to certain functions and to certain networks.

Update License

Access Code information will be displayed on screen. This includes the activation date and the expiration date of the current license. To apply a new license enter the license code. A reboot may be required depending on which license you are applying.

Activation date: December 03 2010
Licensed until: Unlimited

Please use the following Access Code to acquire a new license key from your KEMP representative for your LoadMaster DR.

Access Code: r6w3u-q7w3w-8dd98-72d98

License Key:

System Reboot

Reboot

Reboot the appliance.

Shutdown

Clicking the button attempts to power down the LoadMaster and if for some reason that fails, it will at a minimum halt the CPU.

Reset To Factory Defaults

Reset the configuration of the appliance with exception to the license information and usernames and passwords. This only applies to the active appliance in a HA pair.

Reboot

Shutdown

Reset To Factory Defaults

Update Software

Contact support to obtain the location of firmware patches and upgrades. Firmware download requires Internet access. Detailed patch information is available at <http://forums.kemptechnologies.com/viewforum?f=9>.

Software Update File:

Restore previous version: 1.0-60.20110405-1446

Update Machine

Once you have downloaded the firmware you can browse to the file and upload the firmware directly into LoadMaster. The firmware will be unpacked and validated on LoadMaster. If the patch is validated successfully you will be asked to confirm the release information. To complete the update you will need to reboot the appliance, which can be deferred.

Restore Software

If you have completed an update of LoadMasters firmware you can revert to the previous build.

Backup/Restore

Create a Backup

Generate a backup that contains the Virtual Service configuration and the local appliance information. License information and SSL Certificate information is not contained in the backup.

Restore Configuration

When performing a restore (from a remote machine), the user may select what information should be restored:

The Virtual Service configuration

The LoadMaster Base Configuration

the LoadMaster configuration not including the Virtual Service configuration.

All the configuration information on the LoadMaster.

The screenshot shows two sections on a yellow background. The top section is titled "Create a Backup" and contains a text input field with the placeholder "Backup the LoadMaster DR" and a "Create Backup File" button. The bottom section is titled "Restore Configuration" and contains a "Backup File:" label, a text input field, a "Browse..." button, two checkboxes labeled "LoadMaster DR Base Configuration" and "Geo Configuration", and a "Restore Configuration" button.

Date/Time

You can manually configure the date and time of LoadMaster or leverage an NTP server.

The screenshot shows a configuration table with four rows. Each row has a label on the left and a control on the right. The first row is for "NTP host(s)" with a text input field and a "Set NTP host" button. The second row is for "Set Date" with dropdowns for day (27), month (May), and year (2011), and a "Set Date" button. The third row is for "Set Time" with dropdowns for hour (16), minute (6), and second (21), and a "Set Time" button. The fourth row is for "Set TimeZone" with a dropdown menu set to "UTC" and a "Set TimeZone" button.

NTP host(s)

Specify the host which is to be used as the NTP server. NTP is a strongly preferred option for an HA cluster. For a single unit it is at the user discretion.



The time zone must always be set manually.

Logging Options

Logging of LoadMaster events can be both pushed and also pulled from the appliance. It is important to note that log files on LoadMaster are not historical, if the appliance reboots the logs are reset. It is important to keep a record of events generated on LoadMaster on a remote facility.

Log Files

Boot.msg File contains information during the initial starting of LoadMaster.

Warning Message File contains warnings during the operation of LoadMaster.

System Message File contains system events during the operation of LoadMaster, this included both operating system level and LoadMaster internal events.

Reset Logs will reset ALL log files.

Download all Log Files is used if you need to send logs to KEMP support as part of a support effort. Click this button, save the files to your PC and forward them to KEMP support.

Boot.msg File	<input type="button" value="View"/>
Warning Message File	<input type="button" value="View"/>
System Message File	<input type="button" value="View"/>
Nameserver Log File	<input type="button" value="View"/>
Nameserver Statistics	<input type="button" value="View"/>
Reset Logs	<input type="button" value="Reset"/>
Save all Log Files	<input type="button" value="Download Log Files"/>

Debug options should be used only when directed to do so by KEMP support staff.

Enable IRQ Balance	<input type="button" value="Enable IRQ Balance"/>
Enable Bind Debug Traces	<input type="button" value="Enable Bind Traces"/>
Perform a PS	<input type="button" value="ps"/>
Display Meminfo	<input type="button" value="Meminfo"/>
Display Slabinfo	<input type="button" value="Slabinfo"/>
Perform an Ifconfig	<input type="button" value="Ifconfig"/>
Ping Host	Host: <input type="text"/> <input type="button" value="Ping"/>
Enable IRQ Balance	<input type="button" value="Enable IRQ Balance"/>
Kill VM Instance: 512548	<input type="button" value="Kill VM"/>

TCP dump

Interface: eth0 Address: Port: Start: Stop: Download:

Syslog Options

The LoadMaster can produce various warning and error messages using the syslog protocol. These messages are normally stored locally and may be displayed via the diagnostics menu point. It is also possible to configure the LoadMaster to transmit these error messages to a remote syslog server (menu point: extended->syslog).

Six different error message levels are defined and each message level may be sent to a different server. Notice messages are sent for information only; Emergency messages normally require immediate user action.



One point to note about syslog messages is they are cascading in an upwards direction. Thus, if a host is set to receive WARN messages, the message file will include message from all levels above WARN but none for levels below.



We recommend you do not set all six levels for the same host because multiple messages for the same error will be sent to the same host.

Emergency Host	<input type="text"/>
Critical Host	<input type="text"/>
Error Host	<input type="text"/>
Warn Host	<input type="text"/>
Notice Host	<input type="text"/>
Info Host	<input type="text"/>

 To enable a syslog process on a remote Linux server to receive syslog messages from the LoadMaster, the syslog must be started with the “-r” flag.

SNMP Options

With this menu, the SNMP configuration can be modified.

Enable/Disable SNMP metrics


This toggle option, enables or disables SNMP metrics. I.E. This option allows the LoadMaster to respond to SNMP requests.

 By default SNMP is disabled.

Enable SNMP	<input checked="" type="checkbox"/>
SNMP Clients	<input type="text"/>
Community String	public
Contact	<input type="text"/>
Location	<input type="text"/>
Enable SNMP Traps	<input type="checkbox"/>

Configure SNMP Clients

With this option, the user can specify from which SNMP management hosts the LoadMaster will respond to.

 If no client has been specified, the LoadMaster will respond to SNMP management requests from **any** host.

Configure SNMP Community String

This option allows the SNMP community string to be changed. The default value is “public”.

Configure SNMP Contact

This option allows the SNMP Contact string to be changed. For example, this could be e-mail address of the administrator of the LoadMaster.

Configure SNMP Location

This option allows the SNMP location string to be changed.

SNMP traps

When an important event happens to a LoadMaster a Virtual Service or to a Real Server, a trap is generated. These are sent to the SNMP trap sinks.

Enable/Disable SNMP Traps

This toggle option enables and disables the sending of SNMP traps.

Note: SNMP traps are disabled by default.

Configure SNMP Trap Sink1

This option allows the user to specify a list of hosts to which a SNMPv1 trap will be sent when a trap is generated.

Configure SNMP Trap Sink2

This option allows the user to specify a list of hosts to which a SNMPv2 trap will be sent when a trap is generated.

Email Options

This option permits the configuration of email alerting for LoadMaster events. Email notification can be delivered for six predefined informational levels. Each level can have a distinct email address and each level supports multiple email recipients. Email alerting depends on a mail server, support for both an open relay mail server and a secure mail server is provided. Testing email configuration can be done using the Web User Interface and navigating to System Configuration -> System Administration -> Logging Options -> Email Options

Sample Email Alert:



Oct 22 19:42:16 KEMP2 logger: This is a test from the Load Master

Enable Email Logging	<input checked="" type="checkbox"/>
SMTP Server	<input type="text"/> <input type="button" value="Set Server"/>
Server Authorization (Username)	<input type="text"/> <input type="button" value="Set"/>
Authorization Password	<input type="text"/> <input type="button" value="Set Password"/>
Local Domain	<input type="text"/> <input type="button" value="Set Domain"/>
Emergency Recipients	<input type="text"/>
Critical Recipients	<input type="text"/>
Error Recipients	<input type="text"/>
Warn Recipients	<input type="text"/>
Notice Recipients	<input type="text"/>
Info Recipients	<input type="text"/>
<input type="button" value="Reset"/> <input type="button" value="Change Email Recipients"/>	

Set SMTP Server

Enter the FQND or IP address of the mail server. If you are using FQDN please make sure to set the DNS Server.

Set Authorized User

Enter the username if your mail server requires authorization for mail delivery. This is not required if you mail server does not require authorization.

Set Authorized Users Password

Enter the password if your mail server requires authorization for mail delivery. This is not a required if you mail server does not require authorization.

Set Local Domain

Enter the top-level domain if your mail server is part of a domain. This is not a required parameter.

Set Email Recipient

Enter the email address that correspond with the level or notification desired. Multiple email addresses are supported by a space-separated list, such as:

INFO: info@kemptechnologies.com sales@kemptechnologies.com

ERROR: support@kemptechnologies.com

Miscellaneous Options

Remote Access

Allow Remote SSH Access	<input checked="" type="checkbox"/> Using: All Networks Port: 22 <input type="button" value="Set Port"/>
	Disable SSH-V1 Prot <input checked="" type="checkbox"/>
Allow Web Administrative Access	<input checked="" type="checkbox"/> Using: eth0: 10.200.0.65 Port: 443 <input type="button" value="Set Port"/>
Administrative Default Gateway	<input type="text"/> <input type="button" value="Admin Default Gateway"/>
Radius Server	<input type="text"/> <input type="button" value="Radius Server"/> Shared Secret: <input type="text"/> <input type="button" value="Set Secret"/>
	Revalidation Interval: 60 <input type="button" value="Set Interval"/>
Enable Hover Help	<input checked="" type="checkbox"/>
Enforce Strict IP Routing	<input type="checkbox"/>
GEO LoadMaster Partners	<input type="text"/> <input type="button" value="Set GEO LoadMaster Partners"/>
GEO LoadMaster Port	22 <input type="button" value="Set GEO LoadMaster Port"/>

Allow Remote SSH Access

You can limit the network from which clients can connect to the SSH administrative interface on LoadMaster.

Allow Web Administrative Access

This option allows you to assign the Interface address that will be hosting the Web User Interface access.

Administrative Default Gateway

When administering the LoadMaster from a non-default interface, this option allows the User to specify a different default gateway for administrative traffic only.

RADIUS Server

The address of the RADIUS server that is to be used to validate User access to the LoadMaster. To use RADIUS server you have to specify the shared secret.

Enable hover help

Enables blue hover notes shown when the pointer is held over a field.

Remote GEO LoadMaster Access

Set the addresses of the GEO LoadMasters that can retrieve service status information from this LoadMaster.

GEO LoadMaster Port

The port over which GEO LoadMasters will use to communicate with this LoadMaster unit.

balancing.

L7 Connection Timeout

The number of seconds that all Layer 7 Virtual Services can have no activity, the connection is closed after the timeout is reached.

Always Check Persist

Override the default optimized behavior to only check persistence on initial TCP/IP connection.

A list of files types that should not be cached.

Network Options

Enable Non-Local Real Servers	Yes ▾
Enable Alternate GW support	No ▾
Enable TCP Timestamps	No ▾
Enable TCP Keepalives	Yes ▾
Enable Reset on Close	No ▾
Subnet Originating Requests	No ▾

Enable Non-Local Real Servers

Allow non-local Real Servers to be assigned to Virtual Services.

Enable Alternate GW support

Provides the ability to move the default gateway to a different interface.

Enable TCP Timestamps

The LoadMaster can include a timestamp in the SYN when connecting to Real Servers.



Enable this only upon request from KEMP support.

Enable TCP Keepalives

By default the TCP keepalives are enabled which improves the reliability of TCP connections that are long lived (SSH sessions). Keepalives are not usually required for normal HTTP/HTTPS services.



The keepalive messages are sent from the LoadMaster to the Real Server and to the Client. Therefore, if the Client is on a mobile network, there may be an issue with additional data traffic.

Enable Reset on Close

When enabled the LoadMaster will close its connection with the Real Servers by using RESET instead of the normal close handshake. This only makes a difference under highloads of many connections.

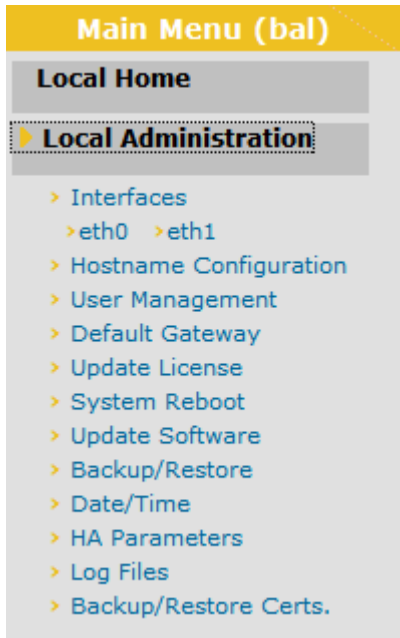
Subnet Origination Requests

When transparency is turned off for a Virtual Service, the source IP address of connections to the Real Servers is the Virtual Service. When enabled, and subnets are being used, the source IP address will be the subnet local address of the LoadMaster. If the Real Server is on a subnet, then the subnet address of the LoadMaster will be used.

HA Parameters

The role of the appliance can be changed by setting the HA Mode. Changing the HA Mode will require a reboot, once LoadMaster has rebooted HA Parameter will appear provided the role is not "Non HA Mode". HA will NOT work if both machines are specified the same.

When logged into the HA pair, use the shared IP address to view and set full functionality to the pair. If you log into the direct IP address of either one of the devices the menu options are dramatically reduced (see menu below). Logging into one of the pair is usually reserved for maintenance



Interfaces





Shared and Partner IP address must be input for the HA cluster to start.

Network Interface 0		
Interface Address (xx.xx.xx.xx[/ss])	10.200.0.65/8	Set Address
HA Shared IP address	10.200.0.70	Set Shared address
HA Partner IP address	10.200.0.69	Set Partner address
Use for HA checks	<input checked="" type="checkbox"/>	
Link Status	Speed: 1000Mb/s, Full Duplex Automatic	Force Link
VLAN Configuration		Interface Bonding
Subnets on this Interface		
Subnet	Local Address	Action
		Add

HA Parameters

HA Status

At the top of the screen, next to the date and time, icons are shown to denote the status of the LoadMaster units in the cluster. There will be an icon for each unit in the cluster. The four possible icons are:

- Green**  The unit is online and operational and the HA units are correctly paired.
- Red/Yellow**  The unit is not ready to take over. It may be offline or incorrectly paired.
- Grey**  The unit is pacified, i.e. it has rebooted more than 3 times in 5 minutes. In this state you can only access the machine via the machine WUI (not the shared WUI), and, it is not participating in any HA activity, i.e. no changes from the master will be received and it will not take over if the master fails.
- Blue**  BOTH machines are active, i.e. both are set to master, and something has gone seriously wrong. **CALL KEMP support.**

HA Mode	HA (First) Mode
HA version	Upgraded (carp)
HA Timeout	9 Seconds
HA Initial Wait Time	0 <input type="button" value="Set Delay"/> (Valid Values: 0, 10-180)
HA Virtual ID	1 <input type="button" value="Set Virtual ID"/> (Valid Values: 1-255)
Switch to Preferred Server	No Preferred Host
HA Update Interface	eth0: 10.200.0.70

In HA mode each LoadMaster will have its own IP address used only for diagnostic purposes directly on the unit. The HA pair have a shared IP address over which the WUI is used to configure and manage the pair as a single entity.

HA Mode

If using a single LoadMaster, select Non-HA Mode. When setting up HA mode, on LoadMaster must be set to HA (First) and the other HA (Second). If they are both set to the same, HA will not operate.



KEMP supplies a license that is HA enabled for each HA unit and specifies first or second unit. Therefore it is not recommended that you change this option until you have discussed the issue with KEMP.

HA Version

By default the system uses a version of VRRP (CARP - Common Address Redundancy Protocol) to check the status of the partner. The systems can also support the legacy heartbeat program. Changes to this option requires both machines to be rebooted for the change to take effect.

HA Timeout

The time that the Master machine must be unavailable before a switchover occurs. With this option, the time it takes an HA cluster to detect a failure can be adjusted from 3 seconds to 15 seconds in 3 second increments. The default value is 9 seconds. A lower value will detect failures sooner, whereas a higher value gives better protection against a DOS attack.

HA Initial Wait Time

How long after the initial boot of a LoadMaster, before the machine decides that it should become active. If the partner machine is running, then this value is ignored. This value can be changed to mitigate the time taken for some intelligent switches to detect that the LoadMaster has started and to bring up the link

HA Virtual ID

When using multiple HA LoadMasters on the same network, this value identifies each cluster so that there are no potential unwanted interactions.

Switch to Preferred Server

By default, neither partner in a HA cluster has priority. So that when a machine restarts after a switchover, the machine becomes slave. Specifying a preferred host means that when this machine restarts, it will always become master and the partner will revert to slave mode.

HA Update Interface

The interface used to synchronize the HA information within an HA cluster.

Inter HA L4 TCP Connection Updates

When using L4 services, enabling updates will allow L4 connections to be maintained across a HA switchover. This option is ignored for L7 services.

Inter HA L7 Persistency Updates

When using L7 services, enabling this option will allow persistence information to be shared between the HA partners. If a HA failover occurs, the persistence information will not be lost. Enabling this option can have a significant performance impact.

Glossary

<u>Access Code:</u>	An Access Code will be generated during the initial setup of the LoadMaster. You must contact your KEMP Technologies representative for your 30-day evaluation license or your full purchased license key.
<u>AFE:</u>	Application Front End, a combination of features which are caching, compression and intrusion prevention.
<u>Balancer:</u>	A network device or logic that distributes inbound connections with a common source address across a farm of server machines.
<u>DR</u>	Disaster Recovery.
<u>Farm Side:</u>	The LoadMaster network interface to which the server farm is connected. I.E. looks 'In' to the internal network
<u>Flat-based:</u>	The VIPs and the Real Servers are defined on the same subnet.
<u>HA:</u>	High Availability
<u>ICMP:</u>	Internet Control Message Protocol
<u>IMAP:</u>	Internet Message Access Protocol
<u>IPS:</u>	Intrusion Prevention System
<u>MAC:</u>	Media Access Control address is a unique identifier assigned to network interfaces for communications on the physical network
<u>MAT:</u>	MAC Address Translation
<u>MIB:</u>	Management Information Base: A database of object definitions (also known as OIDs). Contains the details necessary for an SNMP manager to monitor the objects defined.
<u>NAT:</u>	Network Address Translation
<u>NAT-based:</u>	The request destination IP is modified by the LoadMaster to one of the Real Server IP addresses. Reply traffic from the Real Server must be routed through the LoadMaster so that the reply source IP can be changed to the VIP.
<u>Network Side:</u>	The LoadMaster network interface to which network equipment (router, switch, firewall, etc.) is connected. I.E. looks 'Out' to the internet
<u>One-armed:</u>	Only one Ethernet interface is used for inbound and outbound traffic. (Used interchangeably with Flat-based.)
<u>POP3:</u>	Post Office Protocol (email client protocol)
<u>RS:</u>	Real Server: Physical server machines which make up a server farm.
<u>Service:</u>	A Service is an application that is connected to the network.
<u>Shared IP:</u>	In a LoadMaster HA configuration, the shared (floating) IP address is the "guaranteed available" address for a specific interface (e.g., eth0, eth1).
<u>SCP:</u>	Secure copy command of SSH
<u>SNMP:</u>	Simple Network Management Protocol: A network protocol used to manage TCP/IP networks. This protocol provides functions that enable you to access the data object whose definitions are given by in the MIB.
<u>S-NAT:</u>	Network Address Translation for a source IP address.
<u>SSH:</u>	Secure Shell Protocol.

- Two-armed:* The VIP is defined on a different subnet than the Real Servers.
- UTC:* Universal Time Coordinated (aka GMT).
- VIP:* Virtual IP Address -the IP address of a Virtual Service configured on the LoadMaster.
- VS:* Virtual Service: An entry on the LoadMaster over which a service being hosted in the server farm can be reached.
- WUI:* Web User Interface: Used to perform LoadMaster administration via a web browser.

Index

	A		M
AFE, 28		MAC, 28	
		MIB, 28	
	B		N
Backup, 19			
		NAT, 28	
	C		R
Certificate, 19			
Cluster, 5, 8, 9, 10, 13		Real Server, 28	
		Restore, 18, 19	
	F		S
FQDN, 4, 5, 8, 9, 10, 12, 13, 22			
		SMTP, 22	
	H	S-NAT, 28	
HA, 17, 18, 24, 26, 27, 28		SNMP, 21, 22, 28	
		SSL, 19	
	I		V
ICMP, 16, 28			
IPS, 28		Virtual Services, 24	
	L		
L7, 24, 27			

Document History

Date	Change	Reason for Change	Version	Resp
Jun-11	Added description of new and updated features.	Update manual to match current available software version.	1.0-63	Cmiller