



Virtual Services



August 2021

Contents/Agenda

Goals:

Understand basic Virtual Service
functionality and common deployment
schemes

Virtual Services

Virtual Service is the term for a load balanced, reverse proxy service hosted on the LoadMaster. Each service or series of services are configured to support a specific application or workload.

- Clients will connect to the virtual service, rather than their application server or servers. This helps increase application availability.
- The LoadMaster will determine which server to send each client request to; based on server health checking, advanced scheduling methods and server affinity.

KEMP

LoadMaster

Virtual Services

Home

Virtual Services

Add New

View/Modify Services

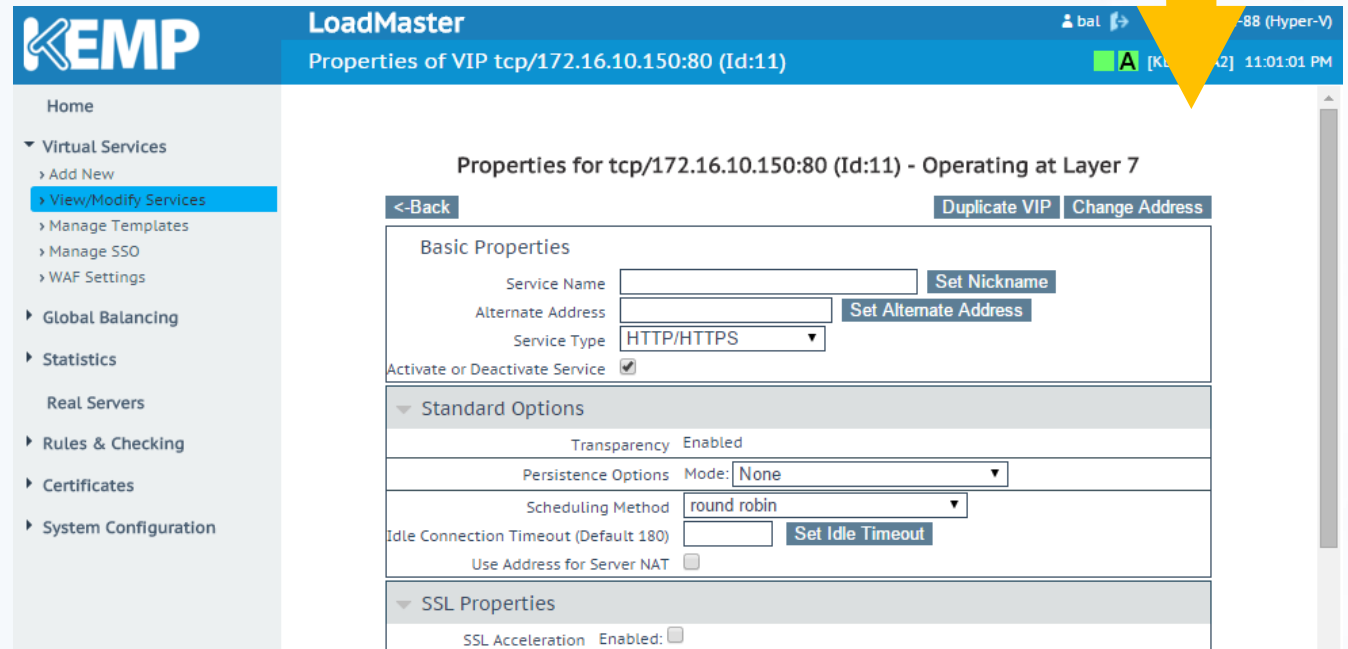
Manage Templates

Manage SSO

WAF Settings

Add New

Virtual IP Address	Prot	Name	Layer	Certificate Installed	Status	Real Servers	Operation
172.16.10.150:80	tcp	HTTP - www.test.com	L7		Down	172.16.10.51 172.16.10.52	<div>ModifyDelete</div>
172.16.10.150:443	tcp	HTTPS - www.test.com	L7	*.test.com	Up	172.16.10.51 172.16.10.52	<div>ModifyDelete</div>
172.16.10.151:3389	tcp	RDP - rdp.test.com	L7		Down	172.16.10.61	<div>ModifyDelete</div>



KEMP LoadMaster

Properties of VIP tcp/172.16.10.150:80 (Id:11)

bal [KEMP] [2] 11:01:01 PM

Properties for tcp/172.16.10.150:80 (Id:11) - Operating at Layer 7

<Back Duplicate VIP Change Address

Basic Properties

Service Name Set Nickname

Alternate Address Set Alternate Address

Service Type HTTP/HTTPS

Activate or Deactivate Service ☒

Standard Options

Transparency Enabled

Persistence Options Mode: None

Scheduling Method round robin

Idle Connection Timeout (Default 180) Set Idle Timeout

Use Address for Server NAT ☐

SSL Properties

SSL Acceleration Enabled: ☐

Virtual Services

It's best to think of a **Virtual Service** as a reverse proxy service, that can offer load balancing, server health checking, security based features and more.

As the ingress point for critical applications, each application may require specific features.

- Server affinity/persistence
- SSL offloading
- Content filtering

Most Commonly Applied VS Features

- Server Health Checking
- Request Scheduling (request distribution)
- SSL Offloading
- Persistence
- Web Application Firewall
- Edge Security Pack
- Content Switching

View/Modify Services

- Provides high level overview of configured virtual services.
 - Virtual Service IP and Port
 - UDP/TCP
 - Service Name
 - L4/L7
 - Certificate information
 - Service Status
 - Server Information

KEMP		LoadMaster						
		Virtual Services						
Home		Add New						
Virtual Services								
Add New								
View/Modify Services								
Manage Templates								
Manage SSO								
WAF Settings								
Virtual IP Address	Prot	Name	Layer	Certificate Installed	Status	Real Servers	Operation	
172.16.10.150:80	tcp	HTTP - www.test.com	L7		Down	172.16.10.51 172.16.10.52	Modify	Delete
172.16.10.150:443	tcp	HTTPS - www.test.com	L7	*.test.com	Up	172.16.10.51 172.16.10.52	Modify	Delete
172.16.10.151:3389	tcp	RDP - rdp.test.com	L7		Down	172.16.10.61	Modify	Delete

- Service status is displayed.
 - Up
 - Disabled
 - Down
 - Fail
 - Redirect
- Server status also displayed.
 - Up == Black
 - Disabled == Orange
 - Down == Red

Creating A New Virtual Service

Add New

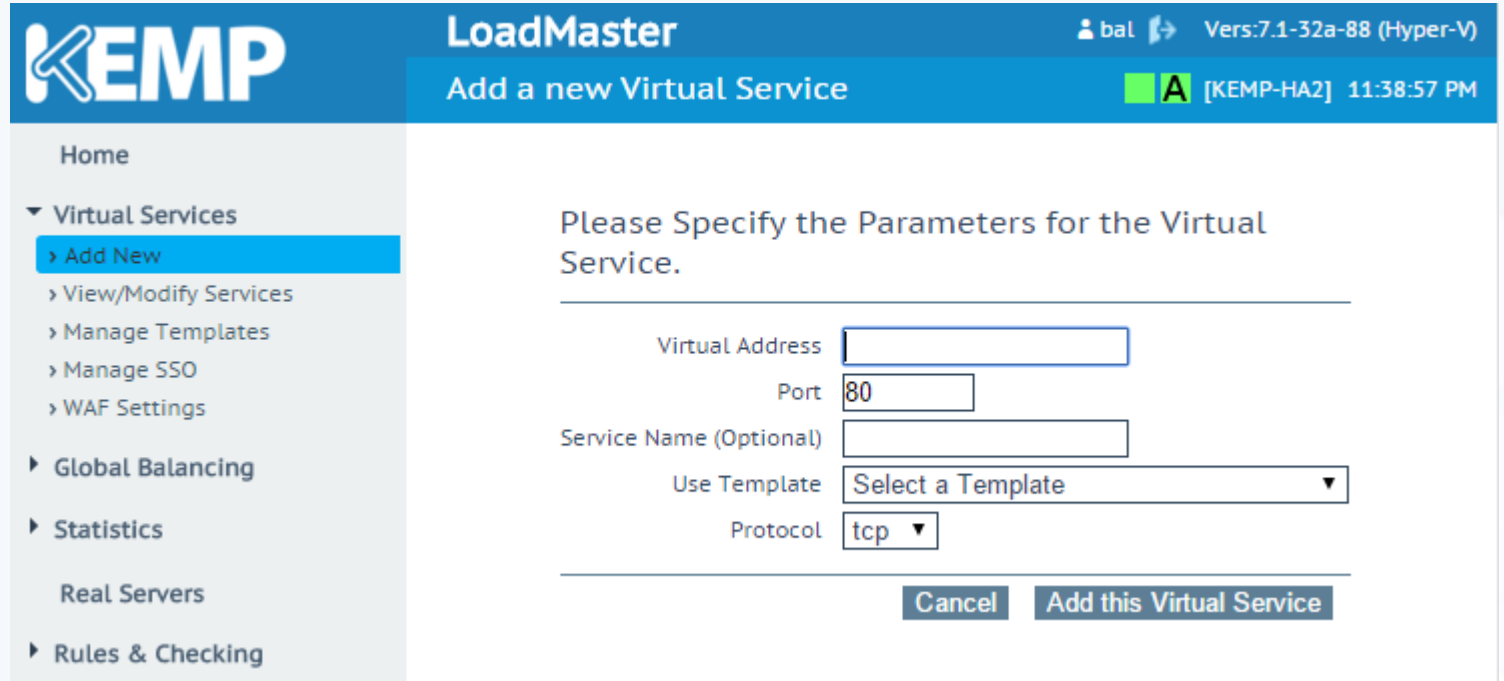
- Used when creating a new virtual service.
- Create a service from scratch or use an Application Template.

Required Initial Settings

- Virtual Service IP address
 - IPv4 or IPv6
 - Must be 'local' IP
 - Unused IP, avoid duplicates
- Virtual Service Port
- Confirm TCP or UDP

Using common protocols/ports will result in displaying specific feature sets and functionality.

- Ex: HTTP, RDP, SMTP, etc.



The screenshot shows the KEMP LoadMaster web interface. The top navigation bar is blue with the KEMP logo on the left, 'LoadMaster' in the center, and user information 'bal' and version 'Vers:7.1-32a-88 (Hyper-V)' on the right. Below the navigation bar, the main heading is 'Add a new Virtual Service'. On the left, a sidebar menu lists various options: 'Home', 'Virtual Services' (expanded), 'Add New' (highlighted), 'View/Modify Services', 'Manage Templates', 'Manage SSO', 'WAF Settings', 'Global Balancing', 'Statistics', 'Real Servers', and 'Rules & Checking'. The main content area is titled 'Please Specify the Parameters for the Virtual Service.' and contains several input fields: 'Virtual Address' (text box), 'Port' (text box with '80' entered), 'Service Name (Optional)' (text box), 'Use Template' (dropdown menu showing 'Select a Template'), and 'Protocol' (dropdown menu showing 'tcp'). At the bottom right of the form are two buttons: 'Cancel' and 'Add this Virtual Service'.

Using Application Templates

- Select Virtual Service IP address
- Select Application Template
- Virtual Service settings will be configured optimally.

Basic Properties

Virtual Service features and options are grouped into broader categories.

- Basic Properties
- Standard Options*
- SSL Properties
- Advanced Properties*
- WAF Options*
- ESP Options*
- Real Servers

*Features vary based on Service Type/protocol.

Properties of VIP tcp/172.16.10.150:80 (Id:1)

A

[KEMP-HA2] 12:08:52 AM

Properties for tcp/172.16.10.150:80 (Id:1) - Operating at Layer 7

<-Back

Duplicate VIP

Change Address

Basic Properties

Service Name

Set Nickname

Alternate Address

Set Alternate Address

Service Type

HTTP/HTTPS

Activate or Deactivate Service

☒

▶ Standard Options

▶ SSL Properties

▶ Advanced Properties

▶ WAF Options

▶ ESP Options

▶ Real Servers

Basic Properties

Service Nick Name

- Only Alphanumeric characters allowed.

Alternate Address

- Creates second listener for virtual service
 - Verify with Netstat
- IPv4 or IPv6 address
- Alternate to creating duplicate virtual service

Service Type

- Allows you to select between groups of protocol specific features.

Activate/Deactive Service – Enable/Disable

Properties of VIP tcp/172.16.10.150:80 (Id:1) ■ **A** [KEMP-HA2] 12:23:45 AM

Properties for tcp/172.16.10.150:80 (Id:1) - Operating at Layer 7

[<-Back](#) [Duplicate VIP](#) [Change Address](#)

Basic Properties

Service Name

Alternate Address

Service Type HTTP/HTTPS ▼

Activate or Deactivate Service

Set Nickname

Set Alternate Address

HTTP/HTTPS

Generic

STARTTLS protocols

HTTP/2

Remote Terminal

Log Insight

▶ Standard Options

▶ SSL Properties

▶ Advanced Properties

▶ WAF Options

▶ ESP Options

▶ Real Servers

Standard Options

Force L7

- Toggle between L4 and L7 service. Visible if no L7 features are being used.

Transparency

- The LoadMaster performs a half NAT, preserving the client's IP address. It uses the client's IP as the Source IP when connecting to the Real Server.
- If enabled, requires the application servers to use the LoadMaster as their default gateway.

Subnet Originating Requests

- When initiating a request to the server, request originates from an interface located on the same subnet as the server.

Standard Options	
Force L7	<input checked="" type="checkbox"/>
Transparency	<input type="checkbox"/>
Subnet Originating Requests	<input type="checkbox"/>
Extra Ports	<input type="text"/> Set Extra Ports
Persistence Options	Mode: <input type="text" value="None"/>
Scheduling Method	<input type="text" value="round robin"/>
Idle Connection Timeout (Default 180)	<input type="text"/> Set Idle Timeout
Use Address for Server NAT	<input type="checkbox"/>
Quality of Service	<input type="text" value="Normal-Service"/>

Standard Options

Extra Ports

- Configures service to listen for traffic on extra port.
- Server will be requested via same port.

Persistence Options

- Provides clients server affinity.
- Options will vary by protocol.
- HTTP/HTTPS have the most options.
 - Cookie based
 - Header based
- Source IP always allowed, but not always optimal.
- Some workloads do not require Persistence.

Scheduling Method

- Dictates which server will receive the next new client request.
- Range from simple to very complex.

Standard Options

Force L7 ☒

Transparency ☐

Subnet Originating Requests ☐

Extra Ports

Set Extra Ports

Persistence Options Mode: **None**

Scheduling Method **round robin**

Idle Connection Timeout (Default 180)

Use Address for Server NAT ☐

Quality of Service **Normal**

SSL Properties

Advanced Properties

WAF Options

ESP Options

Real Servers

Scheduling Method **round robin**

Idle Connection Timeout (Default 180)

Use Address for Server NAT ☐

Quality of Service

SSL Properties

Advanced Properties

WAF Options

ESP Options

Real Servers

Select the type of scheduling of new connections to real servers that is to be performed.

Standard Options

Idle Connection Timeout

- Allows the LoadMaster to close idle connections.
- Global setting applied if left blank.
- 0 – 86400 seconds (1 day)

Use Address For Server NAT

- Only applied to traffic originating from the servers.
 - IE: Connections the server initiates (SYN).
- Server must use LM as default gateway.
- By default SNAT'ed connections will use LM's interface IP address, unless destination port matches the Virtual Service's port, then VS IP is used for SNAT.

Quality of Service

- Adds priority to individual Virtual Services
- Applied to critical applications to avoid latency when the unit is under load.

The screenshot shows the 'Standard Options' configuration page in the Kemp LoadMaster interface. The page is divided into several sections: 'Standard Options', 'Persistence Options', 'Scheduling Method', 'Idle Connection Timeout', 'Use Address for Server NAT', and 'Quality of Service'. The 'Standard Options' section includes checkboxes for 'Force L7' (checked), 'Transparency', and 'Subnet Originating Requests'. There is an 'Extra Ports' input field and a 'Set Extra Ports' button. The 'Persistence Options' section has a 'Mode' dropdown set to 'None'. The 'Scheduling Method' dropdown is set to 'round robin'. The 'Idle Connection Timeout' is set to '1' with a 'Set Idle Timeout' button. The 'Use Address for Server NAT' checkbox is unchecked. The 'Quality of Service' dropdown is open, showing options: 'Normal-Service' (selected), 'Minimize-Cost', 'Maximize-Reliability', 'Maximize-Throughput', and 'Minimize-Delay'. A tooltip on the right says 'Select what Quality of Service should be associated with this VS.' Below the main configuration area are links to 'SSL Properties', 'Advanced Properties', 'WAF Options', 'ESP Options', and 'Real Servers'.

▼ Standard Options	
Force L7	<input checked="" type="checkbox"/>
Transparency	<input type="checkbox"/>
Subnet Originating Requests	<input type="checkbox"/>
Extra Ports	<input type="text"/> Set Extra Ports
Persistence Options	Mode: <input type="text" value="None"/>
Scheduling Method	<input type="text" value="round robin"/>
Idle Connection Timeout	<input type="text" value="1"/> Set Idle Timeout
Use Address for Server NAT	<input type="checkbox"/>
Quality of Service	<input type="text" value="Normal-Service"/>
▶ SSL Properties	
▶ Advanced Properties	
▶ WAF Options	
▶ ESP Options	
▶ Real Servers	

SSL Properties

SSL Acceleration

- “Enabled” allows the LoadMaster to host a certificate to present to clients.
 - LM to server connection is unencrypted.
- “Reencrypt” applies SSL encryption to LM to server connection.
 - This provides end to end encryption, from the client all the way to the server.

Supported Protocols

- Provides granular support for different protocols.

Require SNI Hostname

- Client request must include SNI hostname or connection is reset.

SSL Properties

SSL Acceleration

Enabled: ☒ Reencrypt: ☒

Supported Protocols ☐SSLv3 ☒TLS1.0 ☒TLS1.1 ☒TLS1.2

Require SNI hostname ☐

Certificates

Available Certificates

None Available

Assigned Certificates

Wildcard [*.test.com]

Set Certificates

Manage Certificates

Ciphers

Cipher Set

Default

Modify Cipher Set

Assigned Ciphers

ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA

Client Certificates

No Client Certificates required

Reencryption Client Certificate

None required

Reencryption SNI Hostname

Set SNI Hostname

SSL Properties

Certificates

- Previously imported certificates are listed in the left column. Certificate(s) that have been assigned to this VS are located in right column.
- Certificate's common names evaluated from top to bottom of list against the client's request.
 - If no match, first certificate in the list used.

Cipher Set

- Preconfigured cipher suites, for ease of use.

Ciphers

- Allows inspection of the currently selected ciphers.
- Custom cipher lists are configurable and saved.

The screenshot displays the 'SSL Properties' configuration window. At the top, there are checkboxes for 'SSL Acceleration' (Enabled), 'Reencrypt' (checked), and 'Supported Protocols' (SSLv3, TLS1.0, TLS1.1, TLS1.2). Below these are fields for 'Require SNI hostname' and 'Assigned Certificates' (Wildcard [*test.com]). The 'Certificates' section shows two columns: 'Available Certificates' (None Available) and 'Assigned Certificates' (Wildcard [*test.com]). The 'Cipher Set' dropdown is open, showing a list of cipher suites including Default, Default_NoRc4, BestPractices, Intermediate_compatibility, Backward_compatibility, FIPS, Legacy, Custom_1, and Custom_0. The 'Client Certificates' dropdown is set to 'No Client'. The 'Reencryption Client Certificate' is set to 'None required'. The 'Reencryption SNI Hostname' field is empty. The 'Set SNI Hostname' button is visible. The bottom of the window shows expandable sections for 'Advanced Properties', 'WAF Options', and 'ESP Options'.

SSL Properties

SSL Acceleration Enabled: ☒ Reencrypt: ☒

Supported Protocols ☐ SSLv3 ☒ TLS1.0 ☒ TLS1.1 ☒ TLS1.2

Require SNI hostname ☐

Certificates

Available Certificates: None Available

Assigned Certificates: Wildcard [*test.com]

Set Certificates

Manage Certificates

Cipher Set: Default

Modify Cipher Set

Ciphers

Client Certificates: No Client

Reencryption Client Certificate: None required

Reencryption SNI Hostname: Set SNI Hostname

Advanced Properties

WAF Options

ESP Options

SSL Properties

Client Certificates

- The LoadMaster can pass client certificate information in different formats and through the use of different headers.

Reencryption Client Certificate

- Client certificate hosted by the LoadMaster.

Reencryption SNI Hostname

- Hostname to be named when Client Hello is made.
- Required for ADFS 3.0

SSL Properties

SSL Acceleration

Enabled: ☒ Reencrypt: ☒

Supported Protocols ☐SSLv3 ☒TLS1.0 ☒TLS1.1 ☒TLS1.2

Require SNI hostname ☐

Certificates

Available Certificates

None Available

Assigned Certificates

Wildcard [*.test.com]

Set Certificates

Manage Certificates

Ciphers

Cipher Set

Default

Modify Cipher Set

Assigned Ciphers

ECDHE-RSA-AES256-GCM-SHA384

ECDHE-ECDSA-AES256-GCM-SHA384

ECDHE-RSA-AES256-SHA384

ECDHE-ECDSA-AES256-SHA384

ECDHE-RSA-AES256-SHA

ECDHE-ECDSA-AES256-SHA

Client Certificates

No Client Certificates required

Reencryption Client Certificate

No Client Certificates required

Reencryption SNI Hostname

Client Certificates required

Client Certificates and add Headers

Client Certificates and pass DER through as SSL-CLIENT-CERT

Client Certificates and pass DER through as X-CLIENT-CERT

Client Certificates and pass PEM through as SSL-CLIENT-CERT

Client Certificates and pass PEM through as X-CLIENT-CERT

Advanced Properties

WAF Options

ESP Options

Real Servers

Advanced Properties

Not Available Server

- Treated as a server of last resort, this server will be used if all Real Servers fail health checking.

Default Gateway

- Recommended once the LoadMaster has multiple interfaces assigned. Helps ensure asynchronous routes are not created when responding to end users. Takes priority over global default gateway.

Access Control

- Apply Whitelist/Blacklist rules to the service, configurable for hosts (/32) and entire subnets.

▶ Standard Options

▶ SSL Properties

▼ Advanced Properties

Not Available Server

Port

Set Server Address

Default Gateway

Set Default Gateway

Service Specific Access Control

Access Control

▶ Real Servers

Access Lists for tcp/10.0.7.27:80 (Id:38)

<-Back

Add Blocked Address(es)

IP Address Comment [Block Address\(es\)](#)

Add Allowed Address(es)

IP Address Comment [Allow Address\(es\)](#)



Thank You

kemp.ax