

LoadMaster CLI

Interface Description

UPDATED: 27 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **5**

1.1 Document Purpose 5

1.2 Intended Audience 5

2 LoadMaster Console Operation **6**

2.1 Introduction 6

2.2 Initial Setup 6

2.3 Troubleshooting Licensing Issues 7

2.4 Console Main Menu 8

2.5 Configuration Menu Basics 8

2.6 Main Menu 9

2.7 Quick Setup 10

2.8 Service Management (CLI) 12

2.9 Local Administration 13

2.10 Basic Setup 17

2.11 Packet Filter and Blacklists 18

2.12 Utilities 19

2.13 Reboot 22

3 Command Line Interface (CLI) Reference Guide **23**

3.1 Top level commands 23

3.2 Adaptive scheduling command level 25

3.3 Health Check Command Level 26

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.4 Rules command level 26

3.5 Rule Edit command level 27

3.6 Virtual Service (VIP) command level 29

3.7 Real Server command level 35

References **37**

Last Updated Date **38**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1 Introduction

Kemp leads the industry in driving the price/performance value proposition for application delivery and load balancing to levels that our customers can afford. Our products' versatile and powerful architecture provide the highest value, while enabling our customers to optimize their businesses that rely on Internet-based infrastructure to conduct business with their customers, employees and partners.

Kemp products optimize web and application infrastructure as defined by high-availability, high-performance, flexible scalability, security and ease of management. They maximize the total cost-of-ownership for web infrastructure, while enabling flexible and comprehensive deployment options.

1.1 Document Purpose

This document describes the Command Line Interface (CLI) to the Kemp LoadMaster. It describes in detail how to configure the various features of the Kemp LoadMaster using the CLI.

1.2 Intended Audience

This document is intended to help anyone who wishes to configure the Kemp LoadMaster using the CLI.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2 LoadMaster Console Operation

2.1 Introduction

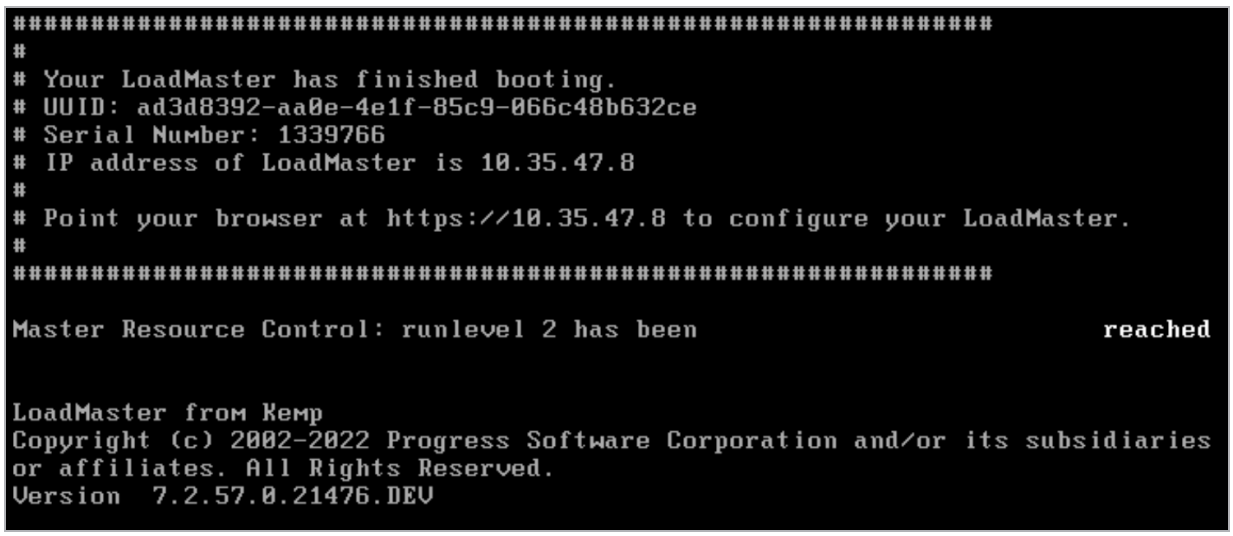
The Command Line Interface allows users to interface with the LoadMaster via a command line shell or a menu-based series of options.

You will need a PC to connect via COM+ (Console) port with a terminal emulation application, or a standard VGA and keyboard. Use a null modem cable (reversal) to connect the COM+ port to the LoadMaster COM port on the rear of the unit.

The COM+ settings should 115200,8,N,1.

Starting with LoadMaster Version 7.2.47, it is possible to connect directly to the LoadMaster serial console in all cloud deployments that support direct serial console access (AWS, for example, currently does not provide direct access to the console). Access to the console allows you to use the CLI and to reset the 'bal' administrative password, as explained in this document. [In previous releases, cloud users could only use the CLI over SSH, and could not use the console to reset the administrative password.]

2.2 Initial Setup



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

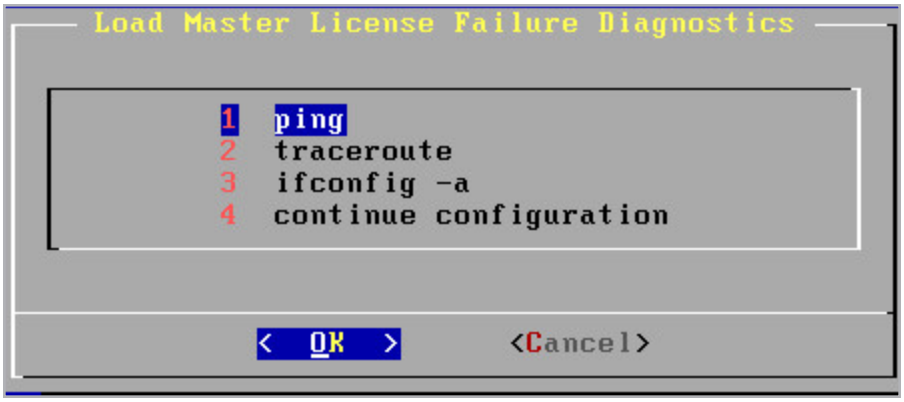
After initially deploying and powering on a LoadMaster, ideally the IP address of the LoadMaster will be obtained via DHCP.

If the IP address has not been obtained via DHCP, or if the address details of the LoadMaster need to be changed, the console can be used to configure the IP address of the LoadMaster, the default gateway address and the name server addresses. To go through this menu, simply log in to the console using the default username and password (**bal** and **1fourall**).

2.3 Troubleshooting Licensing Issues

After configuring the address details and accessing the LoadMaster via the Web User Interface (WUI), the LoadMaster needs to be licensed. For further information on licensing, refer to the Licensing, Feature Description.

If licensing fails for any reason, various debug options will become available on both the WUI and the console. These options can be used to troubleshoot problems which may occur when trying to license the LoadMaster.



If licensing fails for any reason, a diagnostics menu will appear when the LoadMaster console is accessed. This menu has the following options:

- **Ping:** Performs a ping on the specified host. The LoadMaster will try to auto-detect what type of ping to use (ping for IPv4 and ping6 for IPv6). If this auto-detection does not work, you will be asked which ping to use.
- **Traceroute:** Performs a traceroute of the specific host.
- **Ifconfig:** Displays raw ifconfig output.
- **Continue configuration:** Use this option to reconfigure the address details of the LoadMaster.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.4 Console Main Menu

After a LoadMaster has been successfully licensed, the console main menu will be displayed whenever the console is accessed.

If an **SSH Pre-Auth Banner** is set, the banner message is displayed before initially logging in using SSH.

Many features of the LoadMaster can be configured using the menu system. The menu system can be used by logging onto the console as "bal", or by remotely logging into the system using the SSH protocol.

> Remote access is only permitted if the SSH service is enabled and the password for “bal” has been changed from its default value. If the password has not been changed from its default value, the user "bal" will only be allowed to login from a directly connected console.

> As of LoadMaster firmware version 7.2.48.4 Long Term Support (LTS) and 7.2.53, RSA keys are no longer supported for SSH access to the LoadMaster. If you are using RSA keys for SSH access and you are upgrading to one of these versions (or above) you must move to another key type. There are two key types available as an alternative to the RSA keys: ecdsa-sha2-nistp384 and ssh-ed25519

If the password for "bal" has been forgotten, a user can login on the console as **pwreset**. The password is **1pwreset**. This will reset the password for "bal" to **1fourall** until the LoadMaster is rebooted. If unit is rebooted without the password being changed, the password will be reset to its old (unknown) value. It is thus strongly advised that the password should be changed using the configuration menu before the next reboot.

2.5 Configuration Menu Basics

The configuration menu system is made up of a number of hierarchical menus split into functional groups. Navigation around the menus can be performed by using the Up and Down cursor keys, or by using the “+” and “-“ keys. On menus with numeric entries, the number can also be given.

Using “q”<CR> or “ESCAPE” or using the [CANCEL] button will return the user to the previous menu.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

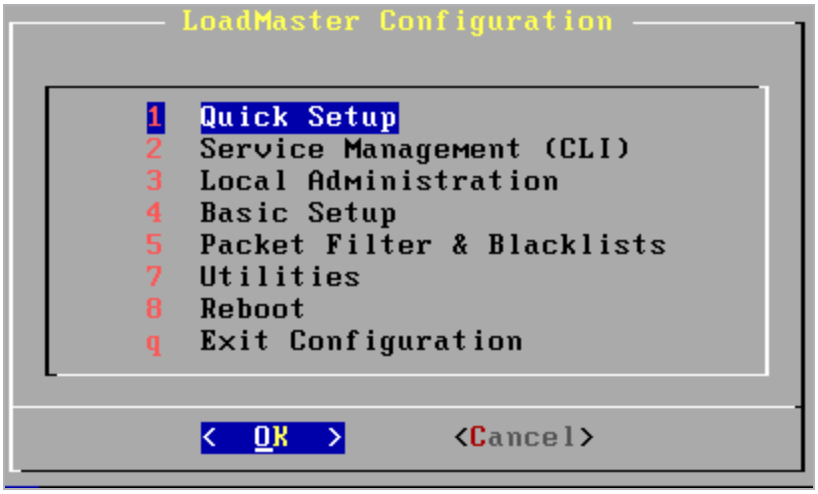
To access the [OK], and [CANCEL] buttons, use the TAB key to toggle between the menu and the buttons.

Using the [CANCEL] button from the main menu, all changes made to the configuration will be ignored.

Using the [OK] button from the main menu performs the menu point, which is currently highlighted.

> When the LoadMaster is configured in a HA cluster, and the user is logged onto the standby machine, only the configuration of the local IP interfaces, changing the local password and performing a backup/restore should be performed, all other configuration parameters should only be changed on the active machine.

2.6 Main Menu



The following options are available on the initial CLI menu.

Quick Setup

Quick setup allows a LoadMaster to be quickly configured; only the most important parameters needed by the LoadMaster are setup.

Service Management (CLI)

This menu point starts a Command Line Interface (CLI), which lets the user administer the Virtual Services that are available on the LoadMaster.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Local Administration

This menu allows you to administrate options such as password, time, backups etc. within the LoadMaster

Basic Setup

From this menu option various aspects of the LoadMaster such as interfaces, hostname, DNS etc. can be configured.

Packet Filter and Blacklists

From this menu Access Control Lists can be administered.

Utilities

A variety of utilities can be administered such as Software Upgrades, determining the Transfer Protocol used, License Updates and configuring a number of diagnostic tools.

Reboot

Selecting the Reboot option enables you to reboot the LoadMaster

Exit Configuration

Exits the menu

These options are discussed in more detail in subsequent sections of this document.

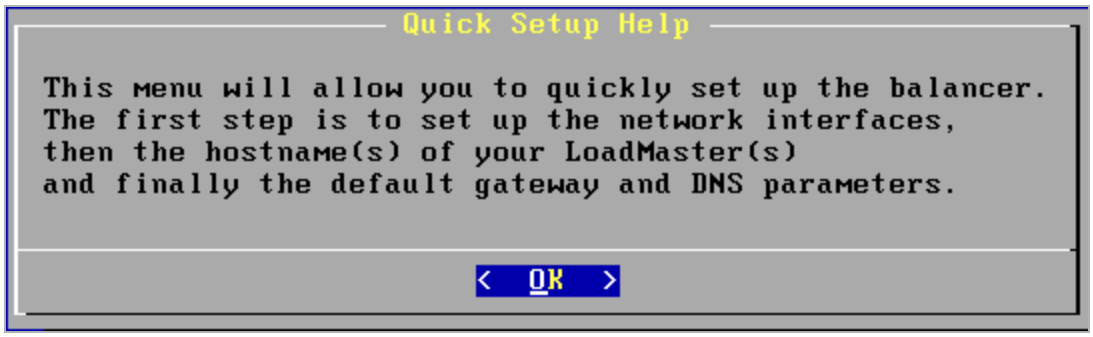
2.7 Quick Setup

Quick setup automatically begins when you log into the LoadMaster for the first time and the license key has been validated. It can also be started by selecting option 1 from the main menu.

Quick setup allows a LoadMaster to be quickly configured; only the most important parameters needed by the LoadMaster are setup. Once the LoadMaster is configured and running, all the parameters can be changed using the Web User Interface.

Quick Setup welcomes you with the following message:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



The Quick Setup procedure allows the configuration of the following parameters:

- Ethernet IP address(s) – for eth0
- Ethernet IP address(s) – for eth1
- Hostname(s) – for local (and partner machine if running in a HA cluster)
- DNS parameters
- Domain parameters
- Default Gateway

After these parameters have been set, the configuration should be activated. The LoadMaster is then ready for use.

> If a parameter has been incorrectly set. Use the [CANCEL] button until the main menu appears. Quick Setup can then be performed again to correct the error.

Ethernet IP address(s) – eth0

The user is asked to input the IP address of the eth0 (NETWORK side) Ethernet interface. This should be input as a “dotted quad” followed by a network specifier.

I.e. 192.168.200.12/24

If no network specifier is given, the user will then be asked to specify the netmask, this may be input as either a network specifier (I.e. for the above example /24.) or as a “dotted quad” (I.e. If the IP address is 192.168.200.12 then the network mask should be 255.255.255.0).

When configuring a HA cluster, the shared IP address will then be requested. This must be on the same network as the primary IP address of eth0 (as previously configured).

Ethernet IP address(s) – eth1

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The user will now be asked to input the IP address of the eth1 (FARM side) Ethernet interface. When running in a Single-Armed configuration, this entry should be left empty.

The format of the input is the same as used for eth0. If an address is given, then this must be on a different network to the address(s) on eth0.

Hostname

The hostname of the LoadMaster must now be set. A standard (or previously set) name is suggested.

When configuring a LoadMaster HA cluster, the name of the partner machine is requested, a standard name is also suggested here. This name also does not need to be changed unless the configuration requires it.

DNS configuration

The DNS resolver may now be configured. Up to three DNS servers may be specified (Addresses must be in “dotted quad” syntax).

A list of search domains can now also be given. Up to 6 domains can be specified.

2.8 Service Management (CLI)

This menu point starts a Command Line Interface (CLI), which lets the user administer the Virtual Services that are available on the LoadMaster.

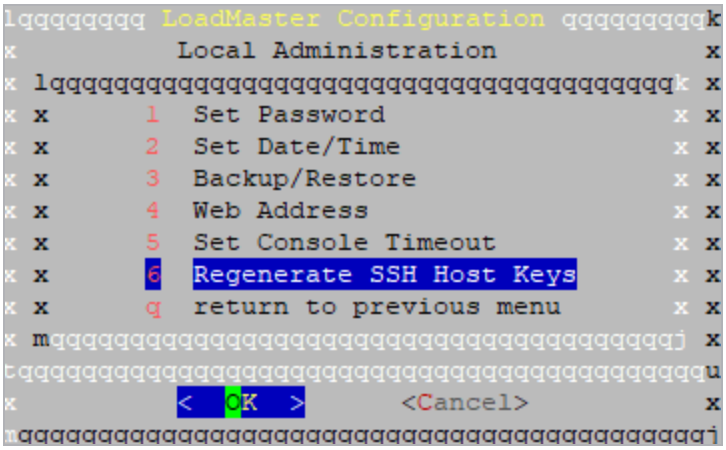


To leave the CLI, the user can type “exit”, or use the ESCAPE or CTRL-D keys.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.9 Local Administration

Selecting option **3**, **Local Administration**, in the Main Menu brings up the **Local Administration** screen.



This menu performs administration tasks for the current LoadMaster balancer. The following options are available:

Set Password

Using this option, the user may change the local password for the user “bal”. The password should be changed for security reasons. Remote access over SSH is not allowed until the password has been changed.

> The password is not saved when performing a backup and is not replaced when performing a restore.

If the LoadMaster is running in a HA (high availability) mode cluster. Each LoadMaster can have a separate password. The password information is not transferred between the members of a cluster.

Set Date/Time

This option allows the local date, time and time zone to be set.

A list of time zones is given; the current time zone is always at the start of the list. The user may select a different time zone if required.

The date should be entered in the following format:

02-12-03 (Year-Month-Day)

Followed by the time in the following format:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

10:57:15 (Hours:Minutes:Seconds)

> When first delivered the LoadMaster is set to use UTC.

Backup/Restore

Selecting the Backup/Restore option is selected a screen opens with two options:

- **Save Backup to Remote Host**
- **Restore Backup from Remote Host**

When option 1 is selected, the backup process begins. The following information is requested:

- The host IP address where the backup will be stored
- The username on the backup host
- The filename of the backup

> The backup server machine must run an FTP daemon or an SSH daemon.

When option 2 is selected, the backup restore process begins. The following information is requested:

- The host IP address where the backup will be stored
- The username on the backup host
- The filename of the backup
- What is to be restored, the options include

    - Only the Virtual Service configuration

    - Only the information about the Virtual Services will be restored.

    - Only the LoadMaster Base Configuration

    - Only the LoadMaster configuration not including the Virtual Service configuration.

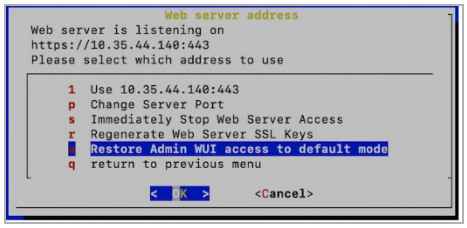
    - Both the Virtual Service and Base Configuration information

    - All the configuration information on the LoadMaster.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> Restoring the Virtual Service Configuration on the standby LoadMaster of a HA cluster is not permitted since the Virtual Service configuration is always taken from the Active LoadMaster, and this would overwrite any restored configuration.

Web Address



The LoadMaster is delivered with the WUI configured to be only accessible via the “network” side address.

When the **Web Address** option is selected, a number of options appear:

- **Use <IP address:Port>:** This displays the IP address which will be used by the LoadMaster WUI. Depending on the value that the IP address is set to, this could be a network side or the farm side IP address. To change the IP address, go to the **Basic Setup** menu item and use the **Network Configuration** option. For more information, refer to the **Basic Setup** section.
- **Change Server Port:** Change the port used by the interface.
- **Immediately Stop/Start Web Server Access:** With this option you can disable or enable access to the LoadMaster WUI.
- **Regenerate Web Server SSL Keys:** This option resets the SSL certificates for the WUI. In a HA environment, the certificates get reset for both the local and shared WUI. Therefore, this needs to be run on both LoadMasters in a HA pair (to remove the local certificate). The certificate on the shared WUI will be corrected on both machines after the first invocation.
- **Restore Admin WUI access to default mode:** Reset the cipher set to the default WUI cipher set (as defined on the **Certificates & Security > Cipher Sets** page). The option **Certificates & Security > Remote Access > Self-Signed Certificate Handling** will also be reset to the default value (**RSA Self-Signed Certs**). This option is designed to restore access to the WUI in the event the cipher settings are misconfigured.
- **Confirm switch out of CC mode:** This option only appears when the LoadMaster is in a specific state. If **Self-Signed Certificate Handling** (in **Certificates & Security > Remote**

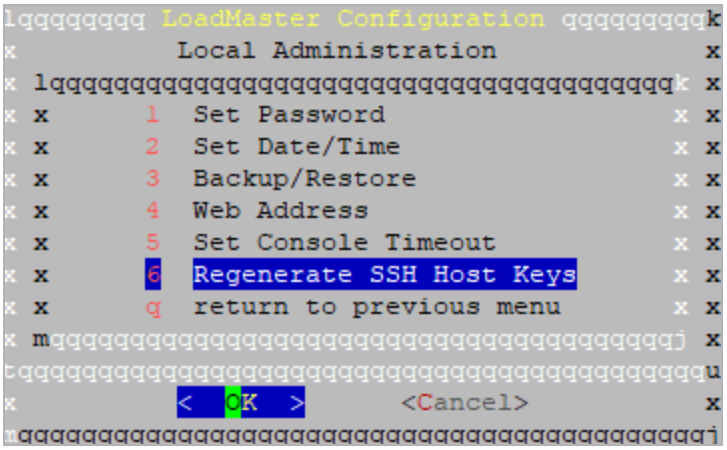
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Access in the WUI) is set to an EC mode and Random Number Generation (RNG) fails (for example, if the hardware does not support it like on legacy systems) a message will display on the home screen saying **Could not start CC mode - system disabled** and the WUI is unusable. This also generates a critical log message saying **Cannot initialize RNG, CC mode disabled** and an authlog saying **Failed to start RNG, CC mode not started**.
To get out of this mode, you must select the **Confirm switch out of CC mode** option. This allows the system to work as usual (but not in Common Criteria (CC) mode).

Set Console Timeout

Use this option to set the idle timeout for the console (in minutes).

Regenerate SSH Host Keys



Host keys are kept in sync on High Availability (HA) machines.

Note that in GEO Partnering mode, SSH host keys are not automatically synchronized, because GEO does not use a shared IP address and the information exchange between partners does not depend on SSH access.

> Amazon Web Services (AWS) sets its own host key so the regenerate SSH host keys functionality is not available on AWS LoadMasters.

> On Azure, there are two authentication mechanisms; password and SSH key. If you have chosen password authentication, it is possible to use the regenerate SSH host keys functionality in the LoadMaster. If you are using Azure SSH key authentication,

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

the regenerate SSH host keys functionality in the LoadMaster is not available.

When you regenerate the LoadMaster's host key, the **$HOME/.ssh/known_hosts** on all current SSH clients must be updated with the new public key.

The SSH key on LoadMaster firmware versions prior to 7.2.51 (or on LTS versions prior to 7.2.48.3) is always the same. When you upgrade to 7.2.51 (or 7.2.48.3 LTS) or downgrade from 7.2.51 (or 7.2.48.3 LTS), the SSH key will change. After upgrading to 7.2.51 (or 7.2.48.3 LTS), the key is regenerated and will stay the same on 7.2.51 (or 7.2.48.3 LTS) and above until you regenerate it again.

2.10 Basic Setup

Selecting the Basic Setup option in the main menu opens the Basic Setup screen



Network configuration

The configuration of the various IP addresses of the Ethernet interfaces can be configured.

When using the LoadMaster in a one-armed configuration, the second interface does not have to be configured. When asked to configure the second interface (eth1) just press the [OK] button with no IP address supplied.

If the LoadMaster is supplied with extra optional Ethernet interfaces, these interfaces can only be configured using this menu. In this case, the on-board interfaces are no longer eth0 and eth1 but the highest numbered Ethernet interfaces. I.e. the optional interfaces will be designated as eth0 and eth1. For more information on this topic please contact customer support.

Hostname Configuration

The hostname of the LoadMaster can be changed. When the system is configured as a HA cluster, the hostname of the partner LoadMaster can also be changed.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

It is not required to change the name of the LoadMaster unless there are multiple HA clusters on the same broadcast network (Ethernet segment).

DNS configuration

This option allows the configuration of the LoadMaster name resolution facility. If no DNS parameters are specified, the administration of the LoadMaster must be performed using “dotted quad” addressing only.

This option allows the configuration of up to three DNS server addresses. These must be in “dotted quad” format.

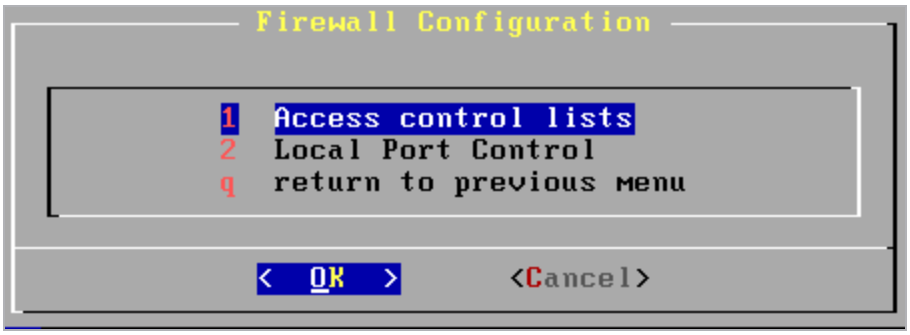
Up to 6 search domains may also be specified.

Default Gateway Configuration

The LoadMaster requires a default gateway through which it can communicate with the Internet. Enter the IP address of the default gateway here. This must be an IP address on the network.

2.11 Packet Filter and Blacklists

Selecting the Packet Filter and Blacklists option from the Main Menu opens the Firewall Configuration screen.



Access Control Lists

The LoadMaster supports a “blacklist” (blocked list) and ‘whitelist’ (allowed list) Access Control List system. Any host or network entered into the blocked list will be blocked from accessing any service provided by the LoadMaster whereas any host or network entered into the allowed list will be allowed to access any service provided by the LoadMaster. The allowed list is used to ‘punch holes’ in the blocked list.

The LoadMaster also has a packet filter. When enabled the packet filter blocks all IP packets which are not directed at a configured port.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The Access Control list is only enabled when the packet filter is enabled. By default the Access Control List is disabled. This means that all source IP addresses are accepted by the LoadMaster.

The following options are available when you select the Access Control Lists option:

- **Enable Access Control Lists:** Using this toggle option the Packet Filter/Access Control List can be activated / deactivated.
- **Show blocked addresses:** This option lists the content of the current blocked list.
- **Add address to blocked list:** This option allows a user to add a host or network IP address to the blocked list. IPv4 and IPv6 addresses are allowed. A network is specified by using a network specifier, i.e. Specifying 192.168.200.0/24 will block all hosts on the 192.168.200 network.
- **Delete address from blocked list:** This option allows an IP address or network to be deleted from the blocked list.
- S**how allowed addresses:** This option lists the content of the current allowed list
- **Add address to allowed list:** This option allows a user to add a host or network IP address to the allowed list.
- **Delete address from allowed list:** This option allows an IP address or network to be deleted from the allowed list.
- **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 LoadMaster may however be configured to send back an ICMP reject packet. For security reasons it is usually best to drop any blocked requests.

2.12 Utilities

Selecting the Utilities option from the Main Menu opens the LoadMaster Utilities screen.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Software Upgrade

Using this option, patches for the operating software of the LoadMaster may be installed or removed. A number of options are available when the Software Upgrade option is selected:

- Install Update

  With this option, a patch can be downloaded onto the LoadMaster from a remote server. The server must be running a SSH daemon.

  Once the patch has been downloaded, the patch is unpacked and verified. If the patch is valid, then the name of the patch will be displayed and the user will be asked to confirm if the patch should be installed. A copy of the current operating software is saved before the patch is installed, this may be recovered at a later date using the “rollback update” option.

- Rollback Update

  If a patch needs to be removed, this option allows the previous version of the operating software to be recovered. Only one previous version is available. When the software has been recovered, it is not possible to recover any earlier versions.

- Factory Reset

  Reset the configuration of the appliance with exception to the license information, usernames and passwords.

Transfer Protocol

This option allows the user to specify which transfer method should be used to transfer data between the LoadMaster and a remote server. The selected method is used to store a backup on a remote server or to download software patches. The default method is “ftp”.

- Use ftp protocol

  Using this option, the Internet standard “ftp” protocol is used. Most servers support this protocol.

- Use scp protocol

  The “scp” - secure copy – transfer method may be selected. This is more secure than “ftp” but is normally only supported on UNIX servers. If this mode is selected, the transfer of SSL certificates can only be performed via the menu system and not via the Web interface.

- Use http protocol

  Using this transfer method, backups to a remote server cannot be performed.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Software patches can however be downloaded from any Web server where the patch has been made available.

License Management

This option permits the input of a new license key, for example, when updating from an evaluation to a full license. Kemp recommends rebooting after updating the license.

Diagnostics

This menu allows the user to perform diagnostic functions on the LoadMaster. The following options are available

- Ping Remote Host

  A remote host may be “pinged”.

- Self Test

  Tests that the Layer 4 and Layer 7 daemons are running correctly

- View Log Files

  Allows the user to view various messages (boot.msg, warning messages, standard messages and the HA logfile) in a terminal view.

- Software Versions

  Displays the software version running on the LoadMaster

- Enable Diagnostic login

  Allows root access to the kernel. An ‘Xroot key’ is also supplied which enables temporary (six hours) xroot access

  > The option “Enable diagnostic login” should only ever be enabled when requested to by LoadMaster support staff.

  If this option is enabled in normal operation, this may result in unauthorized access to the LoadMaster. The diagnostic login will be disabled upon reboot of the LoadMaster or it can be disabled from this menu

- Disable Diagnostic Login

  Disables the Diagnostic Login

- Diagnostic Shell

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Opens a shell from where you can perform diagnostic operations on the LoadMaster kernel.

Telnet can be used as a troubleshooting tool for testing connectivity from within the Diagnostic Shell

> This should only be done with the assistance of a Kemp Engineer

2.13 Reboot

Selecting the Reboot option enables you to reboot the LoadMaster.



If you select the **Yes** option, the LoadMaster reboots.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3 Command Line Interface (CLI) Reference Guide

The command interface syntax is loosely based on the industry standard syntax as used by other Load Balancer manufacturers.

The command interface has a line based, hierarchical command set. Changes made to the configuration are only performed when returning to the top level.

A port can either be specified as a numeric value or as a symbolic name. The following names are recognized:

Protocol	Port
DNS	53
FTP	21
HTTP	80
IMAP4	143
LDAP	389
POP2	109
POP3	110
SMTP	25
SNMP	161
SSL	443
TELNET	23
TFTP	69

3.1 Top level commands

At the top level the following commands may be specified.

Adaptive

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

This command switches the input to the adaptive parameters command set.

Delete <name|VIP>

This command will delete the specified VIP.

Disable_rs <IPspec>

This command will disable the specified Real Server. I.e. No more traffic will be directed to the Real Server. This command will disable the Real Server on all Virtual Services where this Real Server is configured.

Enable_rs <IPspec>

This command will re-enable the specified Real Server. The Real Server will be re-enabled for all Virtual Services.

Health check

This command switches the input to the health check parameter command set.

Rules

This command switches the input to the rule configuration command set. Rules are only available if the L7 option has been activated.

Show <name|VIP>

This command will display all information about the given Virtual Service. If no Virtual Service is specified, information about all Virtual Services will be displayed.

Vip <name|VIP>

This command switches the input to the Virtual Service command set. A <VIP> is the IP address of the Virtual Service. A <name> is the name of the Virtual Service.

If no Virtual Service with the specified IP address (or IP name respectively), then a new Virtual Service will be created. No changes will occur to the configuration until the user returns to the top level command level.

Help

Prints a summary of commands at the current level.

End

Terminate the CLI session.

Exit

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Since the input level is at the top level, this command has no affect.

3.2 Adaptive scheduling command level

The following commands are available at the adaptive command level. No changes to the configuration will occur until the command level returns to the top level i.e. when the user types “exit”.

Interval <Integer>

With this command, the interval of sampling the server loads will be set to <Integer> seconds.

Min <Integer>

The minimum load (as a percentage) where adaptive balancing takes effect can be set.

If the mean load of the server falls below this threshold, the Virtual Service will be considered "idle" and the weights will return gradually to their "static" values.

Port <PortSpec>

The specified port will be used to access the Real Servers where adaptive checking is enabled.

Show

Displays the current adaptive checking parameters.

Url <String>

<String> specifies a URL, which will be fetched by the adaptive checking system. The contents of this URL should specify the load on the current Real Server, with 0 representing no load and 100 representing a fully loaded server.

Weight <Integer>

This specifies the minimal value of the weight (as a percentage of the static weight).

The adaptive scheduling method will not adjust a server weight below this value.

Help

Prints out a list of the available commands at the adaptive command level.

End

Terminates the CLI session. No changes performed after entering this level will be saved.

Exit

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Returns the input to the top command level. Any changes will be written to the configuration file, and the system will be updated accordingly.

3.3 Health Check Command Level

The following commands can be performed at the health check command level. Please note that UDP health checks are not supported via the console.

Interval <Integer>

Specifies how often the health of a Real Server should be checked.

Retry <Integer>

Specifies how often the health check of a Real Server should fail before the LoadMaster decides that the Real Server is no longer responding.

Show

Displays the current health check parameters.

Timeout <Integer>

Specifies how long the LoadMaster should wait for a response from a Real Server. The LoadMaster will mark a Real Server as down after Timeout * Retry seconds if no response has been received.

Help

Lists the commands that are available at the health check command level.

End

Terminate the CLI session. Any changes since entering the health check command level will be ignored.

Exit

Leave the health check command level, any changes to the health check parameters will be saved and the system will be configured accordingly.

3.4 Rules command level

The following commands can be performed at the rules command level.

Add <Rule-name>

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

This command creates a new rule <Rule-name>. It also switches into the Rule Edit command level. Upon return to the Rules command level. Further rules may be added.

A rule must be added before a Real Server can use it.

Modify <Rule-name>

This command switches into the Rule Edit command level, so that the rule <Rule-name> can be edited.

Delete <Rule-name>

This deletes the specified rule. The rule will be deleted from all Real Servers to which it has been assigned.

Show [<Rule-name>]

Displays a list of all the rules (if no <Rule-name> parameter) is specified or the specified rule.

Help

Lists the commands that are available at the rules command level.

End

Terminate the CLI session. Any changes since entering the health check command level will be ignored.

Exit

Leave the rules command level, any changes to the rules will be saved and the system will be configured accordingly.

3.5 Rule Edit command level

The following commands can be performed at the rule edit command level.

value <string>

This option allows the match string value of the rule to be set. Spaces are significant. By default a string is treated as a regular expression. If <prefix> or <postfix> is set, then the string is treated as a literal string, which is then matched at the start or end of the received URL respectively.

[no] negation

This command inverts (reverts to normal if [no] is specified) the sense of a rule. I.e. If negation is set, the rule will be true if the received URL does NOT match the value of the rule.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

[no] prefix

This specifies that the value of the rule should be matched at the start of the received URL.

[no] postfix

This specifies that the value of the rule should be matched at the end of the received URL.

[no] regex+host

This specifies that the value of the rule should be matched against the concatenated hostname and received URL string.

[no] prefix+host

This specifies that the value of the rule should be matched at the start of the concatenated hostname and received URL string.

[**no] postfix+host**

This specifies that the value of the rule should be matched at the end of the concatenated hostname and received URL string.

> If no prefix or postfix option is enabled, the default rule matching will be a regular expression. Specifying **no** to any of the above options reverts the matching back to regular expression matching without any hostname concatenations.

Incquery

Append the query string to the URL before performing a match

Nocase

Ignore case when comparing strings.

Header <string>

The header field name must be matched. If no header field name is set, the default is to match the string within the URL.

Rules can be matched based on the Source IP of the client by entering 'src-ip' within the **Header Field** input field. The header field will be populated by the source IP of the client.

Replacement <string>

The value of the header field to be replaced.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Type <string>

- **Regular Expression:** compares the header to the rule
- **Prefix:** compares the prefix of the header according to the rule
- **Postfix:** compares the postfix of the header according to the rule

Mustfail

If this rule is matched, then always fail to connect.

Onlyonflag <integer>

Only try to execute this rule if the specified flag is se

Setonmatch <integer>

If the rule is successfully matched, set the specified flag

Show

Displays the value of the current rule.

Help

Lists the commands that are available at the rule edit command level.

End

Terminate the CLI session. Any changes since entering the rules command level will be ignored.

Exit

Leave the rule edit command level and return to the rules command level. Modifications will not be saved until after the rules command level is “exited”.

3.6 Virtual Service (VIP) command level

The following commands are available at the Virtual Service command level. No changes will be made to the system until the user performs an “exit” from this level. If the VIP has errors, the user will be asked if the VIP should be discarded. If the VIP is discarded, the input will return to the top level. If the VIP is not discarded, the input will remain at the Virtual Service command level, the user may then correct the error.

[no] Adaptive <String>

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Specifies whether the Virtual Service should support adaptive health checking. The only current method is “http_rs”. To disable adaptive health checking for a Virtual Service, the command <no adaptive> should be used.

Add <IPspec>

This command adds the Real Server as specified by the <IPspec> to the Virtual Service. It also switches the input into the Real Server command level. Upon return from the Real Server command level, further Real Servers can be added to the Virtual Service.

Address <IPspec>

Specifies the IP address of the Virtual Service.

Delete <IPspec>

Deletes a Real Server as specified by <IPspec> from the Virtual Service. A Virtual

Service must have at least one Real Server.

Disable

Disable the Virtual Service. This means that the Virtual Service will accept no new requests.

Enable

Re-enable a Virtual Service. The Virtual Service will again accept new requests.

Follow <Port Spec>

This command only works if the L7 option of the LoadMaster has been enabled. This specifies

Mask <Ipmask>

When using L4 (source IP based persistency), An IP mask may be specified which is used to determine if two IP addresses should be treated as coming from the same source. By default the mask has a value of 255.255.255.255, which means that all IP addresses are different.

[no] Name <Name>

Specifies the “name” of the Virtual Service. To delete the name use the command <no name>.

Healthcheck <String>

This specifies which health-check method should be used for a given Virtual Service. If the Virtual Service has a well-known port, a health check method will be automatically set. The following health check methods may be specified.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Health Check Method	Description
http	HTTP checking is enabled
https	HTTPS (SSL) checking is enabled
smtp	The Simple Mail Transfer Protocol (SMTP) is used.
nntp	The Network News Transfer Protocol (NNTP) is used.
ftp	The File Transfer Protocol (FTP) is used.
telnet	The Telnet protocol is used.
pop3	The Post Office – mail client protocol is used.
imap	The IMAP – mail client protocol is used.
tcp	A basic TCP connection is checked.
dns	A DNS request is sent to the Real Servers port. This checking method is only valid when using a UDP protocol.
udp	A dummy zero length UDP packet is sent to the port.
icmp	An ICMP ping is sent to the Real Server.

Check Parameters

In LoadMaster firmware version 7.2.52, the check **Interval**, **Timeout**, and **Retry Count** settings can be configured on each Virtual Service or SubVS. If any of these parameters are set to 0 they inherit the global value. Previously, these were just global settings

[no] Persist <Persist type>

This command specifies which type of connection persistence should be used for a Virtual Service. In no persistency should be specified for the Virtual Service, the command <no persist> should be specified. The following persistency types can be specified. If the L7 option has not been enabled, only the <src> persistency is allowed.

Persistency type	Description
ssl	The Session ID in an SSL connection is used to maintain client to Real Server persistency.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Persistency type	Description
cookie	Server-generated cookies will be used.
active-cookie	LoadMaster-generated cookies will be used.
url	A request for a specific URL will always go to the same Real Server.
host	A request to the same virtual host will go to the same Real Server.
src	Enables IP-based persistency.
cookie- src	Server-generated cookies will be used. If the client does not return a cookie, the clients' IP address will be used.
active- cook-src	A LoadMaster generated cookie will be used. If the client does not return the cookie, the clients' IP address will be used.
cookie- hash	All connections with the same set of cookies will always be sent to the same Real Server. If no cookies are sent, normal scheduling will occur.

Port <Port spec>

Specifies the IP port to be used for the Virtual Service. If no health check mechanism has been specified and the port is a well-known port, the relevant health check mechanism will be selected.

Precedence <rule-name> <number>

The precedence of the rule <rule-name> is set to <number>. A value of 1 moves the rule to the start of the rule list. I.e. this rule is checked first. A higher value moves the rule to the respective position in the rule. If a <default> rule is specified for a Real Server, its precedence will always be lower than any user defined rules. I.e. a <default> rule will always be checked after every other rule.

Protocol <tcp/udp>

Protocol to be used for the Virtual Service. This may be <tcp> or <udp>. By default the protocol will be set to <tcp>.

Ptimeout <Integer>

Specifies how long the LoadMaster should remember the persistency information associated with a connection. This value is specified in seconds.

Schedule <schedule method>

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

This allows the scheduling method between the Real Servers to be specified.

The following scheduling methods may be specified:

- **rr** round robin (default).
- **wrr**weighted round robin.
- **lc**least connection.
- **llc**weighted least connection.

Server <IPspec>

This command enters the Real Server command level for the specified Real Server.

The Real Server must already be assigned to the Virtual Service.

cache

Enable caching

compress

Enable compression

urlverify

Enable IPS

dfltgw

Configure the VS default gateway

[no] esplog <integer>

Configure what types of logging is allowed

- 0 - Off
- 1 - User Access
- 2 - Security
- 3 - User Access + Security
- 4 - Connection
- 5 - User Access + Connection
- 6 - Security + Connection

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- 7 - All

[no] inauth <integer>

Configure how clients attempting to connect to the LoadMaster are authenticated

- 0 – None: no client authentication is required
- 1 - Basic Authentication: standard Basic Authentication is used
- 2 - Form Based: clients must enter their user details within a form to be authenticated on the LoadMaster

[no] **outauth <integer>**

Configure how the LoadMaster is authenticated by the Real Servers

- 0 – None: no authentication is required
- 1 - Basic Authentication: standard Basic Authentication is used

Note:outauth is restricted by inauth.

Value can only be the same or none.

Form Based auth can use any

Right now the only available option is Basic

addvia <integer>

- 0 - Legacy Operation
- 1 - X-Forwarded-For
- 2 - None
- 3 - X-ClientSide
- 4 - X-ClientSide (No Via)
- 5 - X-Forwarded-For (No Via)
- 6 - Via Only

[no] excludedir [<string>]

List virtual directories specified within this field will not be pre-authorized on this Virtual Service and will be passed directly to the relevant Real Servers.

[no] smtpallow [<string>]

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

List all the permitted domains that are allowed to be received by this Virtual Service

[no] altaddress [<IPspec>]duplicate <IPspec>[no] extraports <integer>[no] sslaccel[no] mtype [<string>]Show

Displays all the parameters of the current Virtual Service.

Help

Prints out a list of commands at the Virtual Service command level.

End

Terminate the CLI session. No changes made in the Virtual Service command level (or lower) will be saved.

Exit

Return the input to the top level. Any changes to the Virtual Service will be saved. If an error is detected in the Virtual Service, the system reports the error and asks if the Virtual Service should be discarded. If the Virtual Service is not discarded, the input remains at the Virtual Service level, where any corrections may be made.

3.7 Real Server command level

At this command level, a specific Real Server may be configured. The following commands are available at this level.

Addrule <Rule-name>

This command adds the rule <Rule-name> to a Real Server. If this is the first assignment of <Rule-name> to a Real Server on the current Virtual Service, the rule will be placed on the precedence list as the lowest user defined rule I.e. checked after all other rules. Use the Virtual Service command Precedence to change the precedence order.

Delrule <Rule-name>

This command removes the association of rule <Rule-name> from the Real Server. If there are no more instances of the rule associated with the Virtual Service, the rule will be deleted from the Virtual Service precedence list.

Disable

Disables the current Real Server. The Real Server will only be disabled in the current

Virtual Service. If the Real Server is accessed via a different Virtual Service, then this

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Virtual Service will not be affected.

Enable

Re-enable the current Real Server on this Virtual Service. If the Real Server has been disabled on multiple Virtual Services, these Virtual Services will not be affected.

Forward <forwarding method>

This specifies the forwarding method, which should be used to access the Real Service.

This can be either <nat> or <route>. By default the forwarding method is <nat>, <route> should only be selected when using “direct service return”.

Port <portspec>

Specifies which port on the Real Server should be used. If no port is specified, then the port from the Virtual Service will be used.

Show

Display the parameters for the current Real Server.

Weight <integer>

Specifies the weighting for the Real Server. This can be used when using the various scheduling methods that utilize the weighting of a Real Server.

Help

Lists the commands at this level.

End

Terminate the CLI session. No changes made in the VIP and Real Server command levels will be saved.

Exit

Return to the Virtual Service command level. No changes will be saved until the editing of the current Virtual Service has been completed.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

References

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

Web User Interface (WUI), Configuration Guide

Kemp LoadMaster, Product Overview

Licensing, Feature Description

RESTful API, Interface Description

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 27 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.