LoadMaster LTS

Release Notes

UPDATED: 06 April 2018

Copyright Notices

Table of Contents

1 Software Release Notes Introduction

This document describes the features in the LoadMaster Long Term Support (LTS) releases.

We recommend you fully back up the LoadMaster configuration before upgrading the software. Instructions for backing up the LoadMaster are described in within the documentation which can be found at http://kemptechnologies.com/documentation.

Installation of this software and reloading of the configuration may take up to five minutes, or possibly more, during which time the LoadMaster being upgraded is unavailable to carry traffic.

1.1 Pre-requisites

The following are recommendations for upgrading the software:

- The person undertaking the upgrade should be a network administrator or someone with equivalent knowledge.
- In case of issues restoring backup configurations, configuring LoadMaster or other maintenance issues, please refer to the LoadMaster documentation which can be found at http://kemptechnologies.com/documentation.

1.2 Support

If there are problems loading the software release, please contact KEMP support staff and a KEMP support Engineer will get in touch with you promptly: http://kemptechnologies.com/load-balancing-support/kemp-support

1.3 Compatible Products

- LM-X15
- LM-X3
- LM-2200
- LM-2400
- LM-2600
- LM-3600
- LM-5300
- LM-5305
- LM-5400
- LM-5000
- LM-5600
- LM-8000
- LM-3000
- LM-4000
- VLM-1000
- VLM-2000
- VLM-5000
- LM for UCS B Series
- LM for UCS C Series
- LM for Oracle Sun x86 servers
- LM for HP ProLiant servers
- LoadMaster for Fujitsu

- LM-8020 (supported on version 7.1-30 and above)
- LM-R320
- VLM-200
- LoadMaster for vCloud Air

Primergy

- LoadMaster for Dell R-Series
- LoadMaster for AWS
- LoadMaster for Azure

2 Release 7.1.35.6 (Long Term Support)

Refer to the sections below for details about firmware version 7.1.35.6.

2.1 7.1.35.6 - Feature Enhancements

- Addressed a critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management where an unauthenticated, remote attacker could bypass security protections, gain system privileges, execute elevated commands, and expose certain sensitive system data, such as certificates and private keys. This vulnerability was partially addressed in 7.1.35.5. The expanded scope of this vulnerability, covering exploitation through injection of arbitrary executable commands in cookies, is addressed in this release.

2.2 7.1.35.6 - Known Issues

PD-10241	Unable to patch upgrade using the Application Program Interface (API) to newer versions of the LoadMaster.
PD-10138	Only text/XML and application/JSON content types are supported with the **Inspect HTML POST Request Content** feature.
PD-10192	The LoadMaster is unable to set up an IPsec tunnel to Azure classic/Azure Resource Manager (ARM) endpoints.
PD-10187	Web Application Firewall (WAF) statistics do not get reset on Virtual Service deletion.
PD-10184	An issue exists which prevents some users from accessing some Virtual Services when using WAF.
PD-10183	WAF does not block the response, even when the **Process Responses** option is enabled on the Virtual Service.
PD-10182	Enabling WAF on a Virtual Service with no rules applied causes a specific web feature to fail.
PD-10181	When an HTTP response contains a status of **HTTP/1.1 500 Internal Server Error** and the location header is populated, the response to the client is dropped and the client sees nothing.
PD-10180	High CPU utilization can be seen when using WAF in certain situations.
PD-9976	An issue occurs preventing Layer7 from initializing when processing SNORT rules.
PD-9953	A security issue exists causing the initial boot password to be written in the Azure Virtual LoadMaster logs.
PD-9777	Issues can occur when using the license API if the timezone on the LoadMaster is set

	to GMT-X.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work on LoadMaster version 7.2.37 and above.
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-9901	HA does not work with LTS VNF 7.1.35.4 on the Multi-Tenant LoadMaster.
PD-9770	ESP logs missing some information.
PD-9743	Issues importing some template files that have the default rule assigned.
PD-9666	Headers with underscores are not accepted by Apache 2.4.
PD-9660	The LoadMaster is changing RADIUS passwords in some scenarios.
PD-9633	Unable to set the check host with the port attached in the WUI (it works using the API or CLI).
PD-9517	Unable to authenticate some users when the password is expired and permitted groups are used.
PD-9508	ESP only verifies SAML assertions when using the root certificate.
PD-9504	Some users are experiencing issues with HA failover on Multi-Tenant LoadMaster units.
PD-10159	CPU and network usage graphs are not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.
PD-9470	LDAP Real Server health checking is not working optimally.
PD-9453	Some Azure users are having issues licensing due to communication issues with the default gateway.
PD-9359	Some users are unable to authenticate using ESP.
PD-9159	When WAF is enabled there is no traffic on the back-end in certain scenarios.
PD-8697	Some users are having issues detecting the partition when using the Hardware Security Module (HSM).
PD-9768	Security issue in the SSO debug logs relating to the logon transcode option.
PD-9657	Naming a cipher set using **-** or **+** results in some issues.
PD-9643	Unable to change the IP address of a Virtual Service in an Azure LoadMaster.
PD-9604	Issues when trying to import some custom templates.

PD-9783	HA status tool tip on slave unit displays incorrect IP addresses.
PD-9758	Some users are unable to edit or access Office files from SharePoint when using SAML and KCD authentication.
PD-7157	When using WAF and KCD, all file attachments in SharePoint fail.
PD-7265	No redirection when the shared IP address is changed using the WUI.
PD-8746	If a LoadMaster licensed with WAF rules has had rules downloaded/installed and then a factory reset is performed, it is not possible to download/install WAF rules.
PD-8413	It is not possible to specify a wildcard port when creating a Virtual Service from a template.
PD-9129	The API command to backup contains an error that breaks the PowerShell wrapper connection.
PD-9779	Discrepancies between the WUI and RESTful API parameter for "Client Authentication Mode".
PD-9596	The **showiface** RESTful API command shows the wrong interface values in the output for interfaces that are not configured.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter values for some RESTful API commands.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9553	There is no API command to disable secure NTP mode.
PD-9539	Issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9525	The RESTful API returns the value of the **failtime** parameter in seconds, but it is set in minutes.
PD-9523	In a specific scenario, the RESTful API returns a success message when fetching a non-existing GEO FQDN.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-7156	The **VSIndex** parameter is missing in some API calls.
PD-9575	There are issues with some **aclcontrol** API commands.
PD-10160	The API commands to reset the CPU and network graphs do not work.

3 Release 7.1.35.5

Refer to the sections below for details about firmware version 7.1.35.5. This was released on 22nd March 2018.

3.1 7.1.35.5 - New Features

The following feature was added to the 7.1.35.5 release:

- Added support for the new LM-X series of LoadMaster hardware.

3.2 7.1.35.5 - Feature Enhancements

- The LTS build is now available in the Azure Marketplace.
- Updated the Copyright Notices on the LoadMaster console and Web User Interface (WUI).

3.3 7.1.35.5 - Issues Resolved

PD-11023	Previously, a critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Now, this vulnerability has been mitigated against with more stringent security checks. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

3.4 7.1.35.5 - Known Issues

PD-10241	Unable to patch upgrade using the Application Program Interface (API) to newer versions of the LoadMaster.
PD-10138	Only text/XML and application/JSON content types are supported with the **Inspect HTML POST Request Content** feature.
PD-10192	The LoadMaster is unable to set up an IPsec tunnel to Azure classic/Azure Resource Manager (ARM) endpoints.
PD-10187	Web Application Firewall (WAF) statistics do not get reset on Virtual Service deletion.
PD-10184	An issue exists which prevents some users from accessing some Virtual Services when using WAF.

PD-10183	WAF does not block the response, even when the **Process Responses** option is enabled on the Virtual Service.
PD-10182	Enabling WAF on a Virtual Service with no rules applied causes a specific web feature to fail.
PD-10181	When an HTTP response contains a status of **HTTP/1.1 500 Internal Server Error** and the location header is populated, the response to the client is dropped and the client sees nothing.
PD-10180	High CPU utilization can be seen when using WAF in certain situations.
PD-9976	An issue occurs preventing Layer7 from initializing when processing SNORT rules.
PD-9953	A security issue exists causing the initial boot password to be written in the Azure Virtual LoadMaster logs.
PD-9777	Issues can occur when using the license API if the timezone on the LoadMaster is set to GMT-X.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work on LoadMaster version 7.2.37 and above.
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-9901	HA does not work with LTS VNF 7.1.35.4 on the Multi-Tenant LoadMaster.
PD-9770	ESP logs missing some information.
PD-9743	Issues importing some template files that have the default rule assigned.
PD-9666	Headers with underscores are not accepted by Apache 2.4.
PD-9660	The LoadMaster is changing RADIUS passwords in some scenarios.
PD-9633	Unable to set the check host with the port attached in the WUI (it works using the API or CLI).
PD-9517	Unable to authenticate some users when the password is expired and permitted groups are used.
PD-9508	ESP only verifies SAML assertions when using the root certificate.
PD-9504	Some users are experiencing issues with HA failover on Multi-Tenant LoadMaster units.
PD-10159	CPU and network usage graphs not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.

PD-9470	LDAP Real Server health checking is not working optimally.
PD-9453	Some Azure users are having issues licensing due to communication issues with the default gateway.
PD-9359	Some users unable to authenticate using ESP.
PD-9159	When WAF is enabled there is no traffic on the back-end in certain scenarios.
PD-8697	Some users having issues detecting the partition when using the Hardware Security Module (HSM).
PD-9768	Security issue in the SSO debug logs relating to the logon transcode option.
PD-9657	Naming a cipher set using **-** or **+** results in some issues.
PD-9643	Unable to change the IP address of a Virtual Service in an Azure LoadMaster.
PD-9604	Issues when trying to import some custom templates.
PD-9783	HA status tool tip on slave unit displays incorrect IP addresses.
PD-9758	Some users are unable to edit or access Office files from SharePoint when using SAML and KCD authentication.
PD-7157	When using WAF and KCD, all file attachments in SharePoint fail.
PD-7265	No redirection when the shared IP address is changed using the WUI.
PD-8746	If a LoadMaster licensed with WAF rules has had rules downloaded/installed and then a factory reset is performed, it is not possible to download/install WAF rules.
PD-8413	It is not possible to specify a wildcard port when creating a Virtual Service from a template.
PD-9129	The API command to backup contains an error that breaks the PowerShell wrapper connection.
PD-9779	Discrepancies between the WUI and RESTful API parameter for "Client Authentication Mode".
PD-9596	The **showiface** RESTful API command shows the wrong interface values in the output for interfaces that are not configured.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter values for some RESTful API commands.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9553	There is no API command to disable secure NTP mode.

PD-9539	Issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9525	The RESTful API returns the value of the **failtime** parameter in seconds, but it is set in minutes.
PD-9523	In a specific scenario, the RESTful API returns a success message when fetching a non-existing GEO FQDN.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-7156	The **VSIndex** parameter is missing in some API calls.
PD-9575	There are issues with some **aclcontrol** API commands.
PD-10160	The API commands to reset the CPU and network graphs do not work.

4 Release 7.1.35.4

Refer to the sections below for details about firmware version 7.1.35.4. This was released on 2nd August 2017.

4.1 7.1.35.4 - Feature Enhancements

- Updated OpenSSH to version 7.5p1
- Improvements made to support a high number of connections.

4.2 7.1.35.4 - Issues Resolved

PD-9678	Fixed an issue that was causing there to be no back-end traffic when the Web Application Firewall (WAF) was enabled.
PD-9650	Fixed an issue that was causing WAF to block the uploading of files larger than 1MB.
PD-9631	It is possible to modify the IP address of the shared IP on a VLAN interface.
PD-9438	Fixed an issue with the **Drop Connections on RS failure** that caused high RAM usage.
PD-9353	Fixed an issue that caused the LoadMaster to reboot when the persistence mode of a UDP syslog Virtual Service was changed.
PD-9352	Fixed an issue that caused simultaneous health check failures.
PD-9333	Removed "deprecated option" SSO manager logs.
PD-9769	Fixed a security issue with the SSO debug logs relating to the logon transcode option.
PD-9637	Mitigated against the CVE-2017-8890 vulnerability.
PD-9756	Fixed an issue with certificate authentication when using a HA pair.
PD-9569	Fixed an issue with special space characters and local LoadMaster user authentication.
PD-9806	Fixed an issue with some **aclcontrol** API commands.
PD-9790	The **CheckPort** and **CheckPattern** API parameters can be unset using the API.
PD-9773	Fixed an issue that showed different statuses for disabled Virtual Services in the API.

4.3 7.1.35.4 - Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass

	security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work on LoadMaster version 7.2.37 and above.
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-9901	HA does not work with LTS VNF 7.1.35.4 on the Multi-Tenant LoadMaster.
PD-9770	ESP logs missing some information.
PD-9743	Issues importing some template files that have the default rule assigned.
PD-9666	Headers with underscores are not accepted by Apache 2.4.
PD-9660	The LoadMaster is changing RADIUS passwords in some scenarios.
PD-9633	Unable to set the check host with the port attached in the WUI (it works using the API or CLI).
PD-9517	Unable to authenticate some users when the password is expired and permitted groups are used.
PD-9508	ESP only verifies SAML assertions when using the root certificate.
PD-9504	Some users are experiencing issues with HA failover on Multi-Tenant LoadMaster units.
PD-10159	CPU and network usage graphs not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.
PD-9470	LDAP Real Server health checking is not working optimally.
PD-9453	Some Azure users are having issues licensing due to communication issues with the default gateway.
PD-9359	Some users unable to authenticate using ESP.
PD-9159	When WAF is enabled there is no traffic on the back-end in certain scenarios.
PD-8697	Some users having issues detecting the partition when using the Hardware Security Module (HSM).
PD-9768	Security issue in the SSO debug logs relating to the logon transcode option.
PD-9657	Naming a cipher set using **-** or **+** results in some issues.

PD-9643	Unable to change the IP address of a Virtual Service in an Azure LoadMaster.
PD-9604	Issues when trying to import some custom templates.
PD-9783	HA status tool tip on slave unit displays incorrect IP addresses.
PD-9758	Some users are unable to edit or access Office files from SharePoint when using SAML and KCD authentication.
PD-7157	When using WAF and KCD, all file attachments in SharePoint fail.
PD-7265	No redirection when the shared IP address is changed using the WUI.
PD-8746	If a LoadMaster licensed with WAF rules has had rules downloaded/installed and then a factory reset is performed, it is not possible to download/install WAF rules.
PD-8413	It is not possible to specify a wildcard port when creating a Virtual Service from a template.
PD-9129	The API command to backup contains an error that breaks the PowerShell wrapper connection.
PD-9779	Discrepancies between the WUI and RESTful API parameter for "Client Authentication Mode".
PD-9596	The **showiface** RESTful API command shows the wrong interface values in the output for interfaces that are not configured.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter values for some RESTful API commands.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9553	There is no API command to disable secure NTP mode.
PD-9539	Issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9525	The RESTful API returns the value of the **failtime** parameter in seconds, but it is set in minutes.
PD-9523	In a specific scenario, the RESTful API returns a success message when fetching a non-existing GEO FQDN.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-7156	The **VSIndex** parameter is missing in some API calls.
PD-9575	There are issues with some **aclcontrol** API commands.
PD-10160	The API commands to reset the CPU and network graphs do not work.

5 Release 7.1.35.3

Refer to the sections below for details about firmware version 7.1.35.3. This was released on 5th April 2017.

5.1 Feature Enhancements

- Updated OpenSSH version to 7.4p1.
- Updated OpenSSL version to 1.0.2k to mitigate against the following vulnerabilities:

  - CVE-2017-3731

  - CVE-2017-3730

  - CVE-2017-3732

  - CVE-2016-7055
- Updated BIND to version 9.10.4-P5 to mitigate against the following vulnerabilities:

  - CVE-2016-9131

  - CVE-2016-9147

  - CVE-2016-9444

  - CVE-2016-9778
- Updated the Copyright Notices on the LoadMaster console and Web User Interface (WUI).
- Support added for OWASP CRS 3.0 rules.

5.2 Issues Resolved

PD-9042	Removed brackets from IPv6 X-Forwarded-For header.
PD-8643	Increased the connection levels that cause local port exhaustion.
PD-8982	Added an option to not include netstat in backups.
PD-9075	Fixed some session management issues.
PD-8996	Fixed an issue that was causing the SSL open/opening connections limit to be reached incorrectly.
PD-8777	Fixed an issue that prevented clients from authenticating using the Edge Security Pack

	(ESP) in certain scenarios.
PD-8717	Fixed an issue relating to the ESP Locked_users file.
PD-8569	Stopped an unnecessary error message from being displayed when viewing log files.
PD-9120	The Virtual Service status is listed in the stats Application Program Interface (API) command.

5.3 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	**Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work on LoadMaster version 7.2.37 and above.
PD-10159	CPU and network usage graphs not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.
PD-8009	The listcluster API command does not return a status.
PD-8298	There are some issues relating to IPv6 routing.
PD-8097	There are some issues accessing WebSocket when using Firefox and a LoadMaster.
PD-8005	There are issues with the PowerShell API that are causing errors with Microsoft Service Management Automation (SMA).
PD-8341	The MTU size is getting reset to 1500 when bonding interfaces.
PD-8305	The aslactivate API command always returns a success message even when the activation fails.
PD-8192	The Get-NetworkDNSConfiguration API command returns High

	Availability (HA) parameters, even when the LoadMaster is not in HA mode.
PD-7778	In some circumstances, the SSL open/opening connections limit is reached, even though there are only a few connections running.
PD-7559	It is not possible to add a comment to a block or whitelist entry in the Access Control List (ACL) when using the API.
PD-8196	There is no validation of the remote URI when enabling WAF logging using the API.
PD-8174	Clusters with a forward slash (/) in the name do not show up in the WUI.
PD-8107	It is not possible to force an NTP update using the API.
PD-8038	In some scenarios, the API is not returning the correct value for the cluster status.
PD-8014	A remote LoadMaster cluster does not respond unless the remote LoadMaster has a Virtual Service.
PD-8225	An incorrect error message is displayed when incorrect credentials are used when licensing the LoadMaster.
PD-8205	When using content rules, the LoadMaster does not match the port when trying to select a Real Server.
PD-7487	When adding a local user and the name of the user is bal, the response is correct but the response stat is invalid – it should be 400/422 or another stat, but not 200.
PD-10160	The API commands to reset the CPU and network graphs do not work.

6 Release 7.1.35.2

Refer to the sections below for details about firmware version 7.1.35.2. This was released on 9th November 2016.

6.1 Issues Resolved

PD-8290	Fixed an issue that was causing browsers to execute JavaScript from warning logs.
PD-8240	Fixed an issue with IP assignment in Azure multi-arm LoadMasters.
PD-8193	Fixed a display issue with statistics.
PD-8189	Fixed an issue that allowed unauthorized API commands to be run.
PD-8188	Fixed an issue that caused errors to appear in the Virtual Service when no Web Application Firewall (WAF) rules were assigned.
PD-8187	Updated BIND to version 9.10.4-P3.

6.2 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8009	The **listcluster** API command does not return a status.
PD-8298	There are some issues relating to IPv6 routing.
PD-8097	There are some issues accessing WebSocket when using Firefox and a LoadMaster.
PD-8005	There are issues with the PowerShell API that are causing errors with Microsoft Service Management Automation (SMA).
PD-8341	The MTU size is getting reset to 1500 when bonding interfaces.

PD-8305	The **aslactivate** API command always returns a success message even when the activation fails.
PD-8192	The **Get-NetworkDNSConfiguration** API command returns High Availability (HA) parameters, even when the LoadMaster is not in HA mode.
PD-7778	In some circumstances, the SSL open/opening connections limit is reached, even though there are only a few connections running.
PD-7559	It is not possible to add a comment to a block or whitelist entry in the Access Control List (ACL) when using the API.
PD-8196	There is no validation of the remote URI when enabling WAF logging using the API.
PD-8174	Clusters with a forward slash (/) in the name do not show up in the WUI.
PD-8107	It is not possible to force an NTP update using the API.
PD-8038	In some scenarios, the API is not returning the correct value for the cluster status.
PD-8014	A remote LoadMaster cluster does not respond unless the remote LoadMaster has a Virtual Service.
PD-8225	An incorrect error message is displayed when incorrect credentials are used when licensing the LoadMaster.
PD-8205	When using content rules, the LoadMaster does not match the port when trying to select a Real Server.
PD-7487	When adding a local user and the name of the user is **bal**, the response is correct but the response stat is invalid – it should be 400/422 or another stat, but not 200.

Last Updated Date

This document was last updated on 06 April 2018.