

LoadMaster 7.2.57.0 Release Notes

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Chapter 2: Before You Upgrade (READ ME FIRST) 6

Supported Models for Upgrade 7

Upgrade Path 8

Upgrade Patch XML File Verification Notes 8

Chapter 3: New Features 9

GEO: BIND Upgrade and EDNS Client Subnet (ECS) Support 9

GEO: Manage FQDN UI Sorting and Filtering 10

GEO: Increase Limit on IPs per FQDN to 256 10

WAF: UI Updates 10

Chapter 4: Change Notices 11

Kubernetes Ingress Controller (KIC): Support for Kubernetes 1.22 11

WAF: Increased Request Body Size Limit 11

WAF: Order of Rule Processing 12

Chapter 5: Security Updates - WAF Engine for CVE-2021-42717 13

Chapter 6: Issues Resolved 14

Chapter 7: New Known Issues 16

Chapter 8: Existing Known Issues 17

1

Introduction

LMOS Version 7.2.57.0 is a feature and bug fix update for the General Availability (GA) branch, made available on 30 June 2022. Please read the sections below before installing or upgrading to this release.

2

Before You Upgrade (READ ME FIRST)

Please pay special attention to the issues below before you begin an upgrade to this release.

Generation of 4096-bit DHE Key

During an upgrade to this version from a version prior to 7.2.53.0, a new 4096-bit DHE key is generated. On some virtual or hardware appliances, this can lead to significant CPU and memory consumption that could impact regular Virtual Service traffic. Progress Kemp strongly recommends that updates to this release from a version prior to 7.2.53.0 be performed during a maintenance interval.

Best Practices Cipher Set

In 7.2.52.0, the **BestPractices** cipher set was updated. If you are upgrading from a version prior to 7.2.52.0, this change is effective immediately after upgrading to this release. This change was made to improve security and conform to the latest industry best practices.

Note: If you depend on any of the cipher sets being removed from the BestPractices set, then *before you upgrade* you must create a custom cipher set that contains these ciphers and assign this new custom cipher set to the Virtual Services that are currently using the BestPractices cipher set. After this is done, you can upgrade to this release and your services will continue to use the old ciphers. If you do not, then after upgrading, any clients that depend on these ciphers being available will no longer be able to connect.

It is recommended, however, that you migrate your services as soon as possible to use the new

BestPractices cipher set.

Related Links

For details, see the following topics:

- Supported Models for Upgrade
- Upgrade Path

Supported Models for Upgrade

This release of LMOS is supported on the Hardware and Virtual models shown in the first three columns of the table below. *It is not supported and should not be installed on any model listed in the column at right.* This update patch can be applied to any supported model regardless of licensing (for example, SPLA, MELA) or platform (for example, hardware, local cloud, public cloud).

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Hardware & Virtual Models	Unsupported Virtual Models
VLM-200	LM-X1	LMB-1G	LM-2000	LM-100
VLM-500	LM-X3	LMB-2G	LM-2200	LM-1000
VLM-2000	LM-X15	LMB-5G	LM-2400	
VLM-3000	LM-X25	LMB-10G	LM-2500	
VLM-5000	LM-X40	LMB-MAX	LM-2600	
VLM-10G	LM-X40M		LM-3500	
VLM-GEO	LM XHC Series		LM-3600	
VLM-MAX	LM-3000		LM-5000	
VLM-SPLA-50	LM-3400		LM-5300	
VLM-SPLA-100	LM-4000		LM-5500	
VLM-SPLA-500	LM-5600		LM-Exchange	
VLM-SPLA-3000	LM-8000		LM-GEO	
VLM-SPLA-GEO	LM-8020		LM-UCS Series	
	LM-8020M		LM-R320	
			LM-5400	

If your model number is not listed above, please see the list of End of Life models.

Upgrade Path

You can upgrade to this release from any previous 7.2.x release. For full upgrade path information, refer to the following article: Firmware Upgrade Path.

Upgrade Patch XML File Verification Notes

By default, verification of the digital signature on upgrade images is required in LMOS 7.2.50.0 and above. See the **Update Verification Options** setting under **System Administration > Miscellaneous Options > WUI Settings**. If the unit you are upgrading is set to require validation, you'll need to supply the XML Verification File supplied with this release.

Note that:

- In previous releases, *two* verification files were provided: one for pre-7.2.51 systems and one for later systems. This restriction has been removed with the 7.2.53.0 release; if upgrading from firmware 7.2.51.0 / 7.2.48.3 and above you can use the XML file provided with this release. If upgrading from any other firmware version you must following the upgrade path detailed in Kemp LoadMaster Firmware Upgrade Path article.
- LoadMasters running an LMOS version prior to 7.2.49 do not provide the option of XML file verification in the UI or API. If you are upgrading from one of these releases to this release, you can verify the digital signatures offline. For further information, refer to the Verifying XML Signatures Technical Note.

Code Signing Certificate Update

On 27 May 2022, the certificate used to sign LoadMaster release artifacts for LoadMaster LMOS version 7.2.56.x and prior releases expired. For most customers, this will not impact normal operations, as explained in this article LoadMaster Code Signing Certificate Expires 27 May 2022.

All LoadMaster releases that occur after the above date (for example, LMOS 7.2.57.0) will be digitally signed using a newly obtained code signing certificate.

3

New Features

Refer to the following sections for details on the new features in this release.

Related Links

For details, see the following topics:

- GEO: BIND Upgrade and EDNS Client Subnet (ECS) Support
- GEO: Manage FQDN UI Sorting and Filtering
- GEO: Increase Limit on IPs per FQDN to 256
- WAF: UI Updates

GEO: BIND Upgrade and EDNS Client Subnet (ECS) Support

BIND is an open source software suite provided by the Internet Systems Consortium (ISC) for interacting with the Domain Name System (DNS). LoadMaster and LoadMaster GEO have been updated to version 9.16.24. BIND 9.16 is the current “Stable/ESV version”, according to the ISC website.

Alongside this update, GEO has been enhanced with Extended DNS (EDNS) Client Subnet, or ECS, support. This is a new global option on the **GSLB Miscellaneous Params** page, which is disabled by default on upgrade and enabled by default on a fresh install. With this feature enabled, GEO will be able to provide better greographic location determination over previous releases.

The ECS feature leverages the larger EDNS packet size and the Client Subnet field that can be set by the client making the DNS request. When a DNS query arrives with an ECS value set, that value will be used as the client location for all DNS operations, with the exception of deny lists. If there is no ECS information in the query (i.e., it was either never supplied by the client or was stripped out by an intervening DNS server that doesn't support EDNS), GEO will behave as in previous releases.

GEO: Manage FQDN UI Sorting and Filtering

The GEO Manage FQDN UI has been enhanced to provide:

- **Sorting**: Controls on the table columns allow for sorting FQDNs by **Name**, **IP Address**, or **Availability**.
- **Filtering**: You can limit the number of FQDNs displayed by selecting one of the **Name** or **IP** address radio buttons at the top right of the table; typing in the text box immediately limits the display to matching FQDNs. These can then be sorted using the controls above. Clearing the text box cancels filtering and displays all items.

GEO: Increase Limit on IPs per FQDN to 256

The number of IP addresses permitted in a single FQDN (Fully Qualified Domain Name) has been increased from 64 to 256. This allows traffic to a single FQDN to be directed to up to 256 endpoints, providing the ability to scale across large load spikes and keep services highly availability.

WAF: UI Updates

The **Web Application Firewall > Access Settings** page of the UI now displays the version of the currently installed OWASP Core Rule Set (CRS).

The **WAF** section of the **Virtual Services Properties** page has been updated to no longer allow individual custom rules to be selected. Custom rule selection is supported on a file basis only.

4

Change Notices

Refer to the following sections for change notices relating to this release.

Related Links

For details, see the following topics:

- Kubernetes Ingress Controller (KIC): Support for Kubernetes 1.22
- WAF: Increased Request Body Size Limit
- WAF: Order of Rule Processing

Kubernetes Ingress Controller (KIC): Support for Kubernetes 1.22

The KIC addon software has been enhanced to support the new Ingress API path element syntax (**networking.k8s.io/v1**) now required by Kubernetes v1.22. The old endpoint (**v1beta**) has been deprecated and is no longer supported with v1.22.

WAF: Increased Request Body Size Limit

In previous releases, the maximum configurable **Request Body Size Limit** for a POST body was 10 MB, with a default of 1 MB. When this WAF option is enabled, any requests that are larger than this limit are

blocked by the WAF engine. The configurable limit has now been increased to 50 MB. This setting is available in a WAF-enabled Virtual Service under **WAF Advanced Options**, when the **Inspect HTTP POST Request Bodies** setting is enabled. Note that increasing the limit above the default of 1 MB will place additional demands on system memory, depending on the number of Virtual Services on which this option is enabled and the level of traffic passing through the Virtual Services.

WAF: Order of Rule Processing

To conform to recommended best practices for using the OWASP Core Rule Set, the order of WAF rule processing has been changed so that custom rule files added by the user are now processed *before* the OWASP CRS rules. In previous releases, the OWASP rules were processed first.

5

Security Updates - WAF Engine for CVE-2021-42717

Refer to the following sections for security updates relating to this release.

The WAF engine has been updated to from ModSecurity 2.9.3 to version 2.9.5 to close the CVE-2021-42717 vulnerability. As a result, a new **JSON Depth Limit** parameter has been added to the **WAF Advanced Options** that controls the depth to which JSON data is examined by the WAF engine. The default of 10000 is the recommended value. Lower values may cause a match failure if not enough data is examined to produce a match; higher values may cause the WAF engine to run slower as the amount of data examined increases.

6

Issues Resolved

PD-19953	**SNMPv2c Walk**: Fixed an issue that caused the SNMP Version 2c Walk command to return no data.
PD-19727	**HTTP/2**: Fixed an internal issue that caused HTTP/2 POSTs to hang indefinitely.
LM-63	**AWS VLM UI**: Fixed an issue that caused the message “Unable to resolve host” to appear on the **Debug Options** page.
LM-67	**Statistics**: Fixed an issue that caused the statd daemon to repeatedly restart when a VXLAN interface is defined with the largest possible VXLAN ID.
LM-69	**WAF and Remote Logging**: When both WAF and Remote Logging are enabled, WAF processing and Layer 7 processing can hang, leading to a service outage. WAF has been modified to continue processing even when log entries are not being processed and a watchdog process will now monitor the logging pipeline to recover remote logging processing if it stops.
LM-80, PD-20101	**Network Telemetry**: Fixed an issue with the 7.2.56.0 version of the Network Telemetry Add-on where flow data is not sent to the Flowmon Collector and the following message appears repeatedly in the system log: flowd: Monitor for interface 0 (pid *xxxxx*) died - exited with status 1
LM-88	**LDAP / LDAPS Health Checks**: Fixed issues that occurred in 7.2.56.0 where LDAP health checks start failing immediately after upgrade, possibly also causing unrelated HTTPS health checks to fail.
LM-92	**Kubernetes Ingress Controller (KIC)**: Fixed an issue where ingress annotations were not working properly because of un-escaped spaces in lists.

LM-104	**Server Side KCD Authentication**: Fixed issues that resulted in users being able to log in despite the failure of KCD due to a misconfiguration (e.g., configured with an invalid domain).
LM-107	**SAML Authentication**: Fixed an issue that caused SSO sessions to be killed by LoadMaster every few hours.
LM-118	**GEO**: Fixed issues that could cause the configuration file generation number and the SOA serial number to become out of sync over time.
LM-581	**UI Certificate Login**: Fixed an issue observed in 7.2.56.0 where enabling UI Remote Access with client certificates *using the API* (not the UI) resulted in login failures.
LM-817	**Single Sign On (SSO)**: Fixed an issue in previous releases where long login delays and authentication failures were observed, typically on units with lower CPU and memory.
LM-934	**Virtual Service Certificate UI**: Fixed an issue in the UI where, when reencryption is disabled, changes to intermediate certificate assignment are not applied.

7

New Known Issues

LM-477	**GEO Downgrade**: When downgrading from a release that supports **more than 64 IPs per FQDN** to a release that only supports **up to 64 IPs per FQDN**, the GEO configuration may become corrupted if there is at least one FQDN in the configuration that contains more than 64 IP addresses. The corruption will likely be evidenced by errors in the UI/API when you list the FQDNs. To avoid this issue entirely, reduce the number of IPs per FQDN to 64 or less for all FQDNs defined *before* you downgrade. If you have already downgraded, you can switch back to the previous boot partition to go back to the newer release (which supports > 64 IPs per FQDN); you can then reduce the number of IPs as above and downgrade again. If neither of these options is possible, please contact Kemp Support who will consult with engineering on a solution to your issues.
LM-864	**GEO Performance**: Starting with LMOS 7.2.55.0, a performance degradation has been seen where Queries per Second (QPS) can be up to 50% lower than with version 7.2.54 and previous releases. This issue will be addressed in the LMOS 7.2.58.0 release.
LM-1134	**GEO EDNS Client Subnet (ECS)**: It has been observed that with ECS enabled and an FQDN with the default private/public behavior selected, a private-network client may receive a non-routable DNS response in certain scenarios.

8

Existing Known Issues

PD-19704	**GEO Cluster Status**: When adding a Cluster that is unavailable (DOWN) to a Site, the Site may reflect the Cluster's status as available (UP) for a short time before changing to DOWN.
PD-19108, LM-127	**GEO**: Modifying an FQDN entry displays a spurious error on the system console, similar to the one shown below. The FQDN is modified properly. <*FQDN*>:794 Uncaught ReferenceError: disp_addrr_elements is not defined at <*FQDN*>:794 (anonymous) @ <*FQDN*>:794
PD-19093, LM-127	**GEO**: Cannot configure GEO into partnering mode unless there is at least one FQDN already defined.
PD-18646, LM-133	**Certificate-Based Administrative Login**: Using a certificate that does not have a SAN attribute (i.e., no Principal Name) results in a failed login attempt.
PD-18615, LM-134	**GEO**: No statistics (queries per second, etc.) are displayed for a site if the FQDN is configured to use the "All Available" Selection Criteria.
PD-18099, LM-136	**Client Certificates**: Authentication may be denied if multiple "Other names" are present in the client certificate.

PD-17927	**LDAP UI Access**: Under certain circumstances, a user that has no LDAP credentials can gain access to the UI.
PD-15872	**LDAP/Syslog**: StartTLS is not working when the **Server Certificate Validation** flag is enabled.
PD-15633	**GEO**: If you add a Zone Name to GEO *after* you have created working FQDNs, GEO may no longer respond to queries for one or more of the FQDNs after the Zone Name is added. The workaround is to remove and then re-add the FQDNs that are no longer working.
PD-15475	**VS Redirects**: If you attempt to upload a new redirect error HTML file to a Virtual Service with **Not Available Redirection Handling** enabled *while traffic is currently being redirected*, then traffic to the VS is dropped. Click the **Error Message** radio button in the UI and the VS begins accepting connections again.
PD-15354	**SSO Timeout**: In LMOS 7.2.51.0, a fix was introduced for issues that caused an SSO client to not be properly logged out when the configured session timeout expires. It has been observed that while sessions do timeout, they are not always closed immediately upon the expiry of the timer; it can take close to a minute longer for the session to be closed.
PD-15294 LM-142	**ESP Verify Bearer Header**: LoadMaster does not return an error when an encrypted token is received and there is no SSL certificate assigned to the VS to decrypt the token.
PD-15172 LM-143	**ESP Verify Bearer Header**: Validation is not working when "Allowed Virtual Hosts" and "Allowed Virtual Directories" are blank on the Virtual Service.
PD-14943	**Single Sign On**: When Form Based Authentication is enabled on the server side, it is possible that after filling out correct credentials and submitting the login form, the form will be presented again; once the second login form is submitted with correct credentials, the login succeeds.
PD-13899	**ACLs and Real Servers**: Real Servers located on networks on which LoadMaster also has an IP address are *always* allowed to access Virtual Services on that network interface regardless of any access control list (ACL) settings on LoadMaster. For Layer 7 services, this issue can be worked around using Content Rules. The workaround for other services is to block access for local Real Servers (if desired) on another network device (firewall, switch, router, etc.).
PD-12838	**ESP / SSO**: The ESP **Permitted Group SID(s)** setting is not working as expected when configured on a SubVS.
PD-12616	**WAF / Compression**: With Web Application Firewall (WAF) enabled, compressed files are incorrectly decompressed. As a workaround, ensure compression is enabled in VS Advanced Properties by selecting the **Enable Compression** option.
PD-12492	**Downgrade**: If an **Azure VLM** is downgraded to the LTS firmware release (7.1.35.x), the WUI may display in the top right-hand corner that the VLM is a **Hyper-V VLM**. This indicates that the **Azure VLM Add-On Package** must be added to the system to provide full Azure VLM functionality. If this occurs, please contact Kemp Support to get the required add-on package.
PD-123	**Hardware Support**: The LoadMaster models LM-X15, LM-X25, and LM-X40 do not support the following

54, PD-10466	SFP+ modules: LM-SFP-SX (SFP+ SX Transceiver 1000BASE-SX 850nm, 550m over MMF), LM-SFP-LX (SFP+ LX Transceiver 1000BASE-LX 1310nm, 10KM over SMF).
PD-12237	**HA / NTP**: Configuring NTP for the first time *after* the system is running in High Availability (HA) mode *and* when the current time on the machines is not correct, may cause the systems to both go into the Master state.
PD-12147	**ESP / RADIUS**: In a LoadMaster configuration with ESP and Radius server-side authentication enabled, sessions may fail to be established.
PD-12058	**Browser Support**: An issue exists when connecting to the LoadMaster WUI when using newer versions of the Firefox browser on initial configuration of a hardware FIPS LoadMaster.
PD-11861	**RADIUS / IPv6**: IPv6 is not supported by the current RADIUS implementation in the LoadMaster for both WUI Authorization and ESP Authentication.
PD-11166	**Networking**: Azure LoadMasters are not translating the additional network address between the Master and Slave correctly.
PD-11044	**SharePoint Virtual Services**: A second authentication prompt is presented when a file is uploaded to SharePoint with the following configuration: WAF is configured with **Process Responses** enabled on the main Virtual Service and KCD is enabled on the SubVS level for server-side authentication.
PD-10917	**HA**: An issue exists when setting up a 2-armed HA Virtual LoadMaster in Azure.
PD-10784	**HA**: Configuring LoadMaster HA using eth1 on an Amazon Web Services (AWS) Virtual LoadMaster does not work.
PD-10490	**WAF**: The *vsremovewafrule* RESTful API command does not allow multiple rules to be removed. This problem has been fixed.
PD-10193	**Exchange 2010 Virtual Services**: A WAF, ESP, and KCD configuration with Microsoft Exchange 2010 is not supported.
PD-10188	**Browser Support**: (Safari) When adding a Real Server to a Virtual Service or SubVS using the Safari browser, the list of available Real Servers is not available.
PD-10159	**Statistics**: When upgrading firmware from version 7.1.35.*n*, CPU and network usage graphs are not appearing. As a workaround, reset the statistics in the WUI.
PD-10136	**Clustering**: In a LoadMaster cluster configuration, a new node can be added with the same IP address as an existing node.
PD-9816, PD-9476	**WAF**: There is an API command to list individual rules in a ruleset, but there is no command to list the available rulesets themselves.
PD-9765	**GEO**: DNS TCP requests from unknown sources are not supported.
PD-9507	**Networking**: Unable to add an SDN controller using the RESTful API/WUI in a specific scenario.

PD-9375	**SharePoint Virtual Services**: Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication.