Progress®
Kemp® LoadMaster®

# LoadMaster 7.2.59.0 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**

Response Code Modification / Filtering . . . . . 9

GEO HTTP HEAD Site Health Checks . . . . . 10

API Updates for WhatsUp Gold Integration . . . . . 11

GEO System Information & Debug Page . . . . . 11

WAF Logging: Splunk HEC Integration . . . . . 13

HTTP Request Load Balancing . . . . . 13

**Chapter 4: Change Notices . . . . . 14**

ACME Support for Multiple Service Providers . . . . . 14

Related API Changes . . . . . 15

Legacy WAF Removed from New Deployments . . . . . 15

**Chapter 5: Security Updates - WAF ModSecurity Engine . . . . . 16**

**Chapter 6: Issues Resolved. . . . . 17**

**Chapter 7: New Known Issues . . . . . 19**

**Chapter 8: Existing Known Issues . . . . . 20**

**Chapter 9: Appendix A: WhatsUp Gold API Integration Example . . . . 25**

# 1

# Introduction

LMOS 7.2.59.0 is a feature and bug fix update for the General Availability (GA) release branch, made available on 27 March 2023. 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 (e.g., SPLA, MELA) or platform (e.g., hardware, local cloud, public cloud).

| Supported Virtual Models | Supported Hardware Models | Supported Bare Metal Models | Unsupported Hardware & Virtual Models |
|---|---|---|---|
| VLM-200 | LM-X1 | LMB-1G | LM-2000 |
| VLM-500 | LM-X3 | LMB-2G | LM-2200 |
| 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 25G | | LM-3600 |
| VLM-MAX | LM XHC 40G | | LM-5000 |
| VLM-SPLA-50 | LM XHC 100G | | LM-5300 |
| VLM-SPLA-100 | LM-3000 | | LM-5500 |
| VLM-SPLA-500 | LM-3400 | | LM-Exchange |
| VLM-SPLA-3000 | LM-4000 | | LM-GEO |
| VLM-SPLA-GEO | LM-5600 | | LM-UCS Series |
| | LM-8000 | | LM-R320 |
| | LM-8020 | | LM-5400 |
| | LM-8020M | | LM-8020-FIPS |
| | | | VLM-100 |
| | | | VLM-1000 |

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 Firmware Upgrade Path article.
- Appliances 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 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:

- Response Code Modification / Filtering
- GEO HTTP HEAD Site Health Checks
- API Updates for WhatsUp Gold Integration
- GEO System Information & Debug Page
- WAF Logging: Splunk HEC Integration
- HTTP Request Load Balancing

## Response Code Modification / Filtering

Response code modification (or filtering) supports the interception of specific HTML response codes received from servers behind LoadMaster and the substitution of another response code and/or text to send back to the client.

This is typically used in an API Gateway deployment to hide back-end responses that might expose sensitive information to a threat actor, and could also be of use to virtually any application.

- Response code modification is a Virtual Service option and is *disabled* by default.
- In the UI, it's located under a Virtual Service's **Advanced Settings**.
- Click **Show Text & Mappings** to display the response code modification configuration. Note that:
  - The configuration can be edited before enabling the **Response Code Modification** check box.
  - If any mappings have been configured, the button text will show the number of HTML response codes that have been mapped.
- On the **HTTP Response Code Management** page, there are two accordions:
  - **Response Text** shows the text returned to clients along with the response code. The default is the standard HTML response code text and can be edited. Blank text is not allowed.
  - **Response Mappings** shows the currently mapped response codes; by default, this table is empty. Use the controls provided to map one or more server HTML response codes to a single code to be returned to clients.

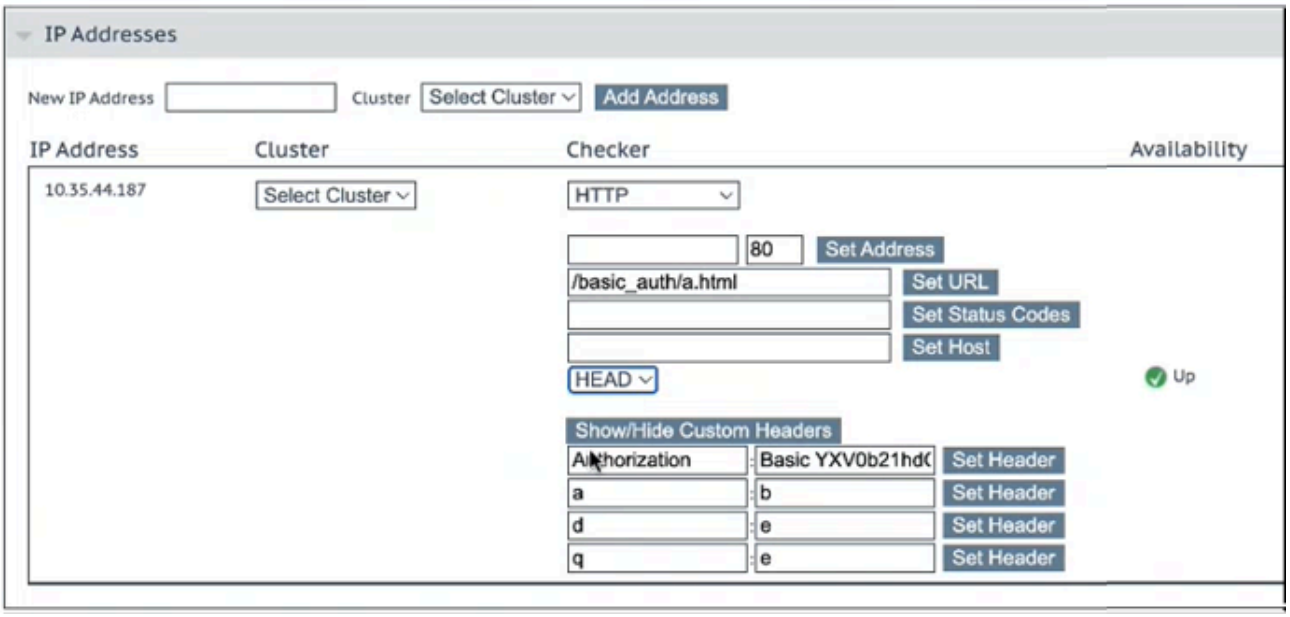
**Limitation**: Any HTML response code that specifies a redirect (300-399) is *only* intended to be intercepted on the way from the server and a substitute response code returned to the client. There is no provision for specifying a redirect URL to send to the client.

# GEO HTTP HEAD Site Health Checks

GEO site health checking has been expanded to include the HTTP HEAD method. This can be useful for many different application types. The following configuration options are supported:

- Specify the name and content of a specific header to provide to the application.
- Up to 4 custom headers can be defined per GEO Site.
- The status of the last health check performed is reflected in the UI and log.
- Return codes of 200-299, 301, 302, and 401 are interpreted to mean the server is healthy.

The following example shows how to configure an HTTP HEAD check to authenticate to the site using basic authentication via the Authorization header. The header value is “Basic”, followed by a space, followed by a base64-encoded string.




# API Updates for WhatsUp Gold Integration

The LM *accessv2/* API endpoint has been enhanced to improve LoadMaster integration with WUG and similar API-based monitors.

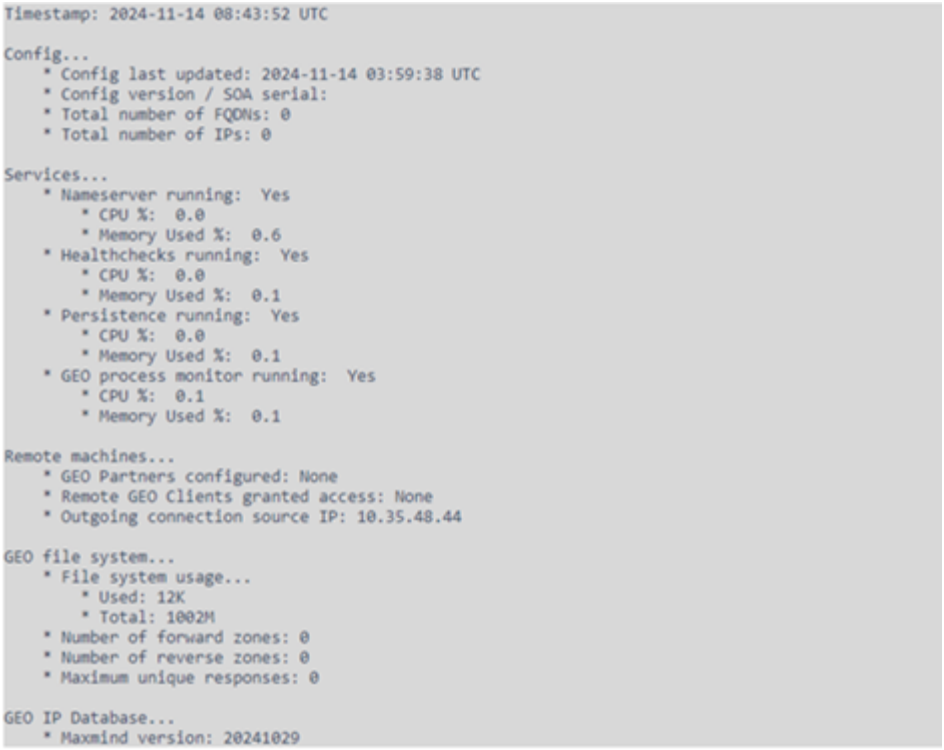
- Input data can be provided in either of two ways:
  - Using a POST of JSON-format data (as in previous releases)
  - Inline in the URL using a GET command
- Basic authentication can be provided using the "Authorization" header.

This makes it possible to configure a WhatsUp Gold monitor to leverage the *accessv2/* API and plot graphs on the WhatsUp Gold console using data returned by the API. An example would be using the LM API stats command to graph VS stats like *totalbytes* and *bytespersec*. See Appendix A: WhatsUp Gold API Integration Example for an example.

# GEO System Information & Debug Page

A new **Global Balancing > GEO System Info / Debug** page provides the following status information to aid in troubleshooting DNS issues:

- GEO Configuration
- DNS Services
- Partners & Clients
- File System Stats
- GEO IP DB version



```
Timestamp: 2024-11-14 08:43:52 UTC

Config...
    * Config last updated: 2024-11-14 03:59:38 UTC
    * Config version / SOA serial:
    * Total number of FQDNs: 0
    * Total number of IPs: 0

Services...
    * Nameserver running:  Yes
        * CPU %:  0.0
        * Memory Used %:  0.6
    * Healthchecks running:  Yes
        * CPU %:  0.0
        * Memory Used %:  0.1
    * Persistence running:  Yes
        * CPU %:  0.0
        * Memory Used %:  0.1
    * GEO process monitor running:  Yes
        * CPU %:  0.1
        * Memory Used %:  0.1

Remote machines...
    * GEO Partners configured: None
    * Remote GEO Clients granted access: None
    * Outgoing connection source IP: 10.35.48.44

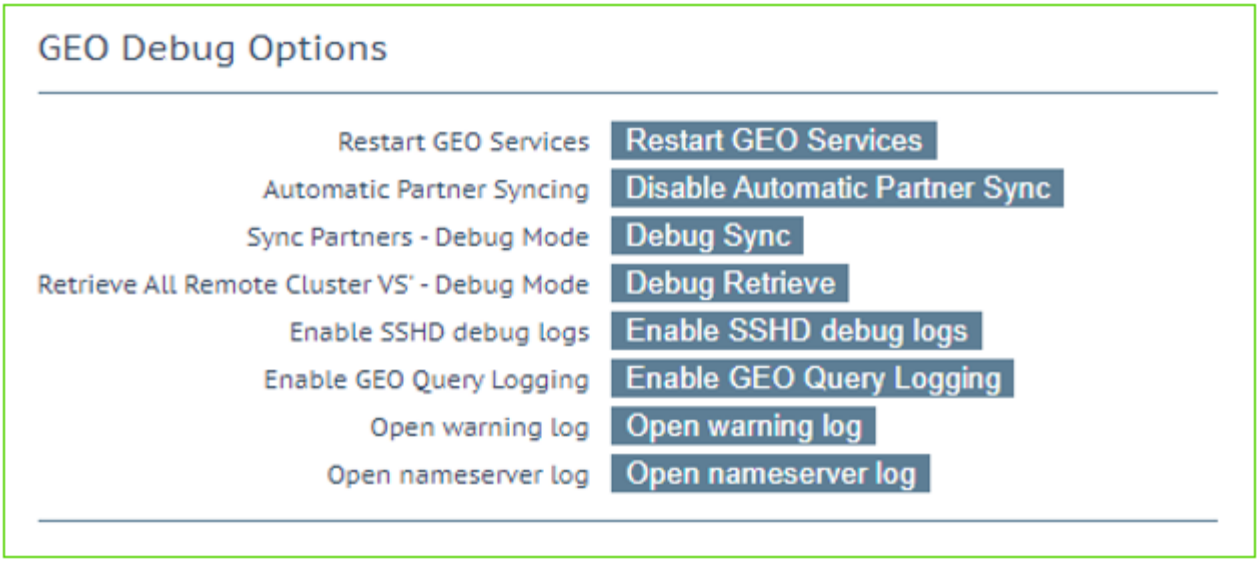
GEO file system...
    * File system usage...
        * Used: 12K
        * Total: 1002M
    * Number of forward zones: 0
    * Number of reverse zones: 0
    * Maximum unique responses: 0

GEO IP Database...
    * Maxmind version: 20241029
```

In addition, new **GEO Debug Options** are provided at the bottom of the page:

- Manually restart all GEO services.
- Enable/disable partner syncing. Disabling it may be useful when debugging complex environments. While its disabled, the manual sync button still operates.
- Manually sync GEO partners using verbose debug logging.
- Retrieve status of all remote cluster Virtual Services using verbose debug logging.
- Open logs (without having to go to the logging UI).
- Enable debug logging for SSH connections.
- Enable debug logging for DNS queries.

Most of these options should be used with caution and only to debug specific issues for a limited period of time. Debug logging, for example, can consume a significant amount of system resources while enabled.




# WAF Logging: Splunk HEC Integration

To respond to customer requests for increased availability of LM logs to 3rd party SIEM products, WAF logging has been enhanced to support integration with Splunk via the HTTP Event Collector (HEC):

- A new Splunk Logging Format is supported for JSON remote logging, which is only displayed when the Enable Remote Logging check box is enabled.
- LM logs have been enhanced to be displayed properly by Splunk.
- Note that a SPLUNK username is used to authenticate to HEC, along with an HEC authentication token.
- A new Logging Format is supported for JSON remote logging, which is only displayed when the Enable Remote Logging check box is enabled.
- A hard-coded SPLUNK username is used to authenticate to HEC, along with an HEC authentication token.
- The Password/Token must be obtained from the HEC configuration.

# HTTP Request Load Balancing

LoadMaster by default performs 'connection-based load balancing' – meaning that although many http requests are pipelined into a single connection, load balancing is performed using the information associated with the first request in the connection only.

Some customers with specific application demands require instead 'request-based load balancing" where *each request* in a connection is load balanced separately from other requests.

HTTP request-based load balancing is disabled by default and can be enabled using the **Reschedule on every HTTP Request** check box in a Virtual Service's **Advanced Properties**. This can be used in combination with any of the **Selection Methods** supported under **Standard Options**, but *should not be used with HTTP/2 workloads*.

# 4

# Change Notices

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

**Related Links**

For details, see the following topics:

- ACME Support for Multiple Service Providers
- Related API Changes
- Legacy WAF Removed from New Deployments

## ACME Support for Multiple Service Providers

The current ACME-client-based support for automated certificate management has been enhanced to support using *both* LetsEncrypt and DigiCert as an ACME Certificate Authority (CA) in the same deployment. In previous releases, only certificates from one CA could be managed.

If you have certificates from an ACME CA before you upgrade, those certificates are preserved. After upgrade, the UI page for selecting a CA re-appears; select your current CA provider to see your current certificates.

# Related API Changes

The following changes have been made to the API to improve its usability across multiple CAs.

**In LMOS 7.2.58.0**, all ACME parameters are managed via set and get commands using these parameters:

- directoryurl
- renewperiod
- kid
- hmac

**In LMOS 7.2.59.0** and subsequent releases:

1. Each parameter above has it's own get/set command.
2. For all ACME commands, a new required parameter (`acmetype`), specifies the CA to which the command applies:
   - 1 = LetsEncrypt
   - 2 = DigiCert

Here are syntax summaries for the new API commands:

**`setacmedirectoryurl`**`?directoryurl=`*`value`*`&acmetype={1|2}`
**`setacmerenewperiod`**`?renewperiod=`*`value`*`&acmetype={1|2}`
**`setacmekid`**`?kid=`*`value`*`&acmetype=1`
**`setacmehmac`**`?hmac=`*`value`*`&acmetype=1`

**`getacmedirectoryurl`**`?acmetype={1|2}`
**`getacmerenewperiod`**`?acmetype={1|2}`
**`getacmekid`**`?acmetype=1`
**`getacmehmac`**`?&acmetype=1`

# Legacy WAF Removed from New Deployments

The deprecated Legacy WAF functionality no longer appear on Virtual Services in new deployments of 7.2.59.0. Upgrades to 7.2.59.0 will preserve Legacy WAF functionality; be advised, however, that the Legacy WAF functionality will be removed in an upcoming release. If you are still using Legacy WAF, we recommend that you upgrade to using the latest WAF functionality as soon as possible.

# 5

# Security Updates - WAF ModSecurity Engine

The ModSecurity engine has been updated to the version 2.9.6:

- This version closes a serious security vulnerability in how SQL commands are constructed, as detailed in https://nvd.nist.gov/vuln/detail/CVE-2022-39956.
- Additional fixes in version 2.9.6 that are unrelated to CVE-2022-39956 are listed in the ModSecurity release notes.

# 6

# Issues Resolved

| | |
|---|---|
| LM-2252 | **GEO**: Fixed an issue that caused a segmentation fault when a DNS Time Signature (TSIG) record is received. [Note: TSIG records are ignored by GEO.] |
| LM-2251 | **Certificate Authentication**: Fixed an issue (introduced in 7.2.56.0) where certificate login is failing with an audit log message incorrectly indicating that the certificate Subject Alternative Name (SAN) field doesn't contain a User Principle Name (UPN). |
| LM-2239 | **Kubernetes Ingress Controller (KIC)**: Fixed an issue where under certain circumstances Real Servers are not added as expected to a Virtual Service. |
| LM-2073 | **Kubernetes Ingress Controller (KIC)**: Fixed an internal issue that caused adding Virtual Services to fail. To address these issues, upgrade to 7.2.59.0 and update the KIC add-on packages to the 7.2.59.0 versions. |
| LM-1900 | **GEO**: Fixed an issue wherein using the **All Available** selection criteria can cause the name resolution daemon (*named*) to consume additional resources and provide unexpected responses. |
| LM-1881 | **SAML Authentication**: Fixed an internal error that could cause SAML decoding to fail with a message similar to this:<br><br>`ssomgr: auth_saml_post: ERROR SAML Response decode failed!` |
| LM-1803 | **Kubernetes Ingress Controller (KIC)**: Fixed an issue where upgrading the KIC add-on can result in the duplication of SubVSs. |
| LM-1735 | **GEO**: Fixed an issue where GEO is disabled but spurious logs and alerts appear warning about the failure of GEO processes. |

| | |
|---|---|
| LM-1723 | **GEO Partnering**: There is a small window of time during a partner sync where concurrent changes on the partners may not be reflected on both systems. The only workaround is to repeat the modification. |
| LM-1715 | **WAF**: Fixed a bug that caused only Legacy WAF custom rules to be displayed in the UI when WAF is *not* enabled on any Virtual Service. |
| LM-1369 | **Single Sign ON (SSO)**: Fixed an issue that caused SSO logins to not be blocked after the configured number of failed attempts. |
| LM-1281 | **Kubernetes Ingress Controller (KIC)**: Fixed an issue where enabling LDAP for UI login results in errors like the following when Kubernetes attempts to contact LoadMaster via the API:<br><br>`validuser: bind failed for user [k8s] ...` |
| LM-1038 | **Single Sign On w/Permitted Groups**: Fixed an intermittent issue where the wrong permitted group may be chosen on login. |
| LM-662 | **GEO**: In previous releases, Cluster Checks can be selected even when there are no clusters present. This UI issue has been fixed. |
| LM-99 | **ACME Lets Encrypt Certificates**: In previous releases, Lets Encrypt certificates could not be deleted even when not being used. This issue has been fixed. |

# 7

# New Known Issues

| | |
|---|---|
| LM-2505 | **GEO**: GEO stops responding to DNS requests when the **Weighted Round Robin** selection method is used. The workaround is to use Round Robin instead. This issue will be addressed in a May 2023 update. |
| LM-2470 | **GEO**: Starting with 7.2.59.0, a segmentation fault may be observed when GEO processes a DNS PTR record. This issue will be addressed in a May 2023 update. |
| LM-2398 | **Kubernetes Ingress Controller (KIC)**: A real server deleted from the UI is not added back by KIC. |
| LM-2396 | **API**: On the KVM platform only, the *getall* API call fails. |

# 8

# Existing Known Issues

| | |
|---|---|
| LM-2566 | **Layer 7 Persistence**: Enabling the **Always Check Persist** option in a Virtual Service breaks server cookie persistence for that Virtual Service. The only workaround is to disable **Always Check Persist**. |
| LM-2034 | **GEO**: Starting with 7.2.55.0, using the Real Server Load selection criteria may result in no traffic being processed. |
| LM-1865 | **WAF Audit Logs**: No output is returned when selecting a date range. |
| LM-1809, LM-1800 | **Azure VLM**: Disk usage in the logging partition (*/var/log/*) may increase because of files used by the Azure agent (*waagent*) process that are never removed. Users that experience this issue will need to call support for a workaround. |
| LM-1557 | **Single Sign On**: A segmentation fault in the SSO management process can occur under high load resulting in users being logged out. Messages like the following will be seen in the log:<br>`kernel ssomgr[46119]: segfault at <num> ip <num> sp <num> error 4`<br>`kernel L7: verify_user: Auth request failed for id 0` |
| LM-1527 | **GEO Cluster Checks**: GEO cluster checks against LoadMasters configured in Clustering mode do not work. |
| LM-1412 | **API stats command**: On a unit in Clustering mode, the up/down status value returned via the stats command may be different (and incorrect) compared to the status returned by listvs or vstotals. |
| LM-137 | **Let's Encrypt ACME Certificates**: After certificate renewal, the old certificate may still be in use by the |

| | |
|---|---|
| 3 | Virtual Service. The workarounds are to either:<br>• Remove and re-add the Virtual Service certificate<br>• Disable and re-enable the Virtual Service |
| LM-1342 | **Kubernetes Ingress Controller**: Ingress may stop working if the default admin gateway is modified. The workaround is to return the setting to the old gateway address. |
| LM-1325 | **Let's Encrypt UI**: The UI for requesting a new certificate may not fully load with a large number of Virtual Services configured. The workaround is to use the API. |
| 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.<br>To avoid this issue entirely, reduce the number of IPs per FQDN to 64 or less for all FQDNs defined *before* you downgrade.<br>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.<br>If neither of these options is possible, please contact Kemp Support who will consult with engineering on a solution to your 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.<br><*FQDN*>:794 Uncaught ReferenceError: disp_addrr_elements is not defined<br>at <*FQDN*>:794<br>(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-180 | **Client Certificates**: Authentication may be denied if multiple "Other names" are present in the client |

| | |
|---|---|
| 99, LM-136 | 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<br>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<br>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-12354, PD-10466 | **Hardware Support**: The LoadMaster models LM-X15, LM-X25, and LM-X40 do not support the following 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-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. |

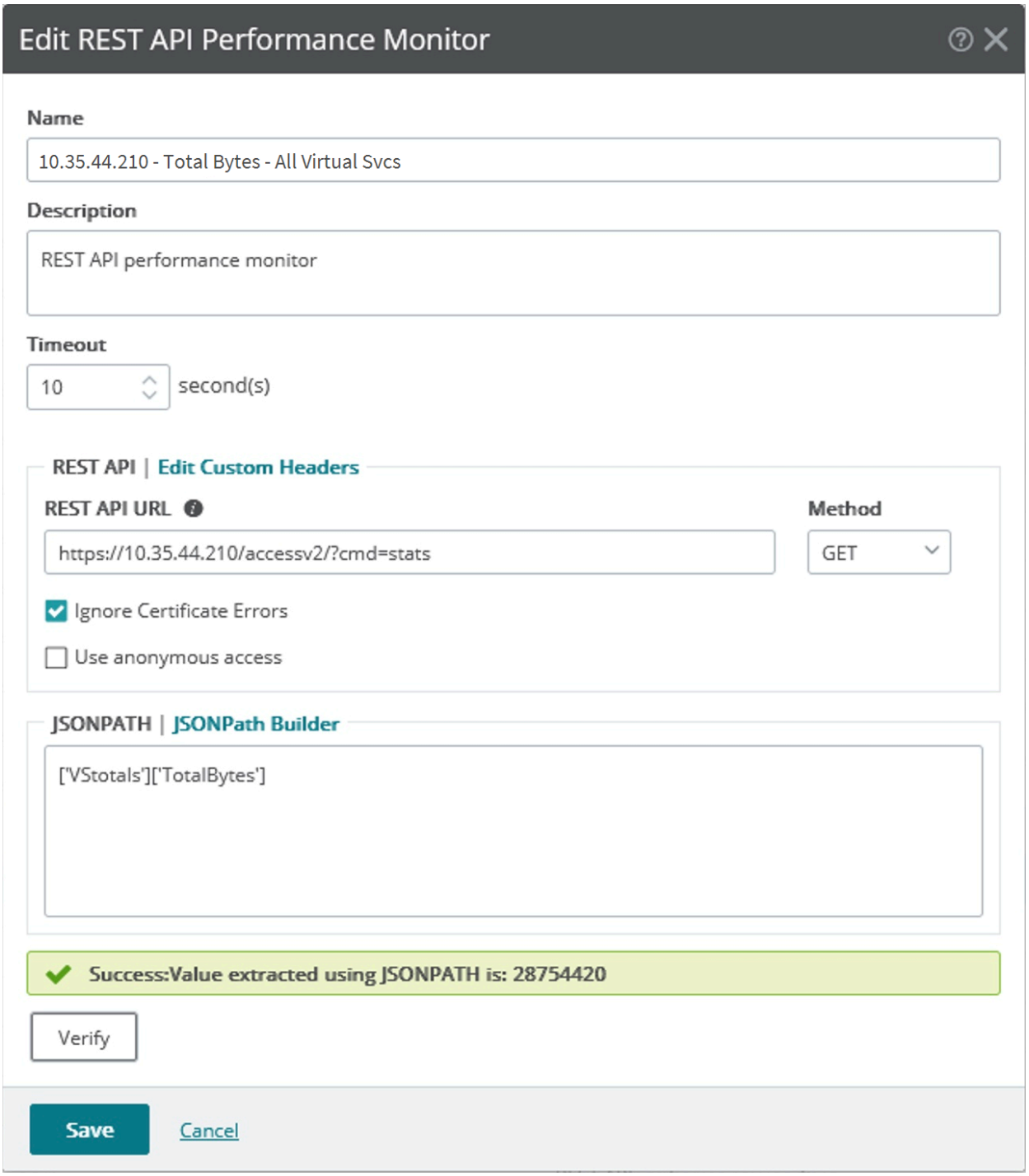
| | |
|---|---|
| PD-9375 | **SharePoint Virtual Services**: Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication. |

# 9

# Appendix A: WhatsUp Gold API Integration Example

To configure a WhatsUp Gold monitor for a LoadMaster, do the following:

1. Log in to WhatsUp Gold and open the **My Network** tab.
2. Select your LoadMaster from the device list and click on **Properties** in the upper right corner.
3. Select the “+” button and then navigate to **Performance monitor-> Create**.
4. Select the **Rest API** monitor type.
5. Fill in the form:
6. Be sure to specify the **accessv2/** endpoint in the **REST API URL.**
7. The **Method** must be **GET**.
8. In the **JSONPATH** field, provide the path to the data point(s) in the LoadMaster API's **stat** command JSON output to monitor. The following is what your screen should look like before saving.




9. Click **Verify** to test your settings.
10. Click **Save**.