Progress®
Kemp® LoadMaster®

LoadMaster 7.2.58.0 Release Notes

Generated on: 16 September 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

ACME Support for DigiCert SSL Certificate Management 9

Virtual Service Sorting 10

Virtual Service Filtering 11

Duplicating a Sub Virtual Service (SubVS) 11

Chef Template and Deployment Guide 11

DataDirect Template and Deployment Guide 12

License Mobility 12

Chapter 4: Change Notices 13

GEO: Ignore ECS for Public/Private Decisions 13

WAF PCRE Limit Enhancements 14

Official Support for VMware 7.0 Update 3d 14

Chapter 5: Security Updates 15

Weak Ciphers Removed from FIPS Cipher Set 15

FIPS Mode Cipher Sets Modified to Remove Less Secure Ciphers 16

Upgrade: Removed Ciphers in Custom Cipher Sets 16
Local User Certificate Login Behavior Switch 17

Chapter 6: Issues Resolved 18

Chapter 7: New Known Issues 20

Chapter 8: Existing Known Issues 22

1

Introduction

LMOS 7.2.58.0 is a feature and bug fix update for the General Availability (GA) release branch, made available on 27 October 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 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 Announcement on the Support website.

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:

- ACME Support for DigiCert SSL Certificate Management
- Virtual Service Sorting
- Virtual Service Filtering
- Duplicating a Sub Virtual Service (SubVS)
- Chef Template and Deployment Guide
- DataDirect Template and Deployment Guide
- License Mobility

ACME Support for DigiCert SSL Certificate Management

Broadens the current ACME-client-based support for automated certificate management to support DigiCert as an ACME Certificate Authority:

- Each LoadMaster can be associated with a specific DigiCert account by setting various account parameters and communicating with DigiCert servers to confirm the settings.
- Administrators will be able to request and renew DigiCert certificates from the LoadMaster UI.
- The DigiCert account cannot be created (nor funds added to it) from the LoadMaster UI. An account must be requested through the DigiCert website and already exist so that the appropriate configuration parameters can be entered into the LoadMaster UI.
  - Since DigiCert is a paid service, sufficient funds must be added to your account *before* requesting certificates via the LoadMaster UI.
- The UI has been updated to generalize the text used in menus and labels and to provide new pages for DigiCert account and certificate management. Similarly, the API has been updated to provide generalized calls. Backward compatibility is maintained for the previous LE-specific calls.
- The main UI menu has a new sub-menu, **ACME Certificates**, replacing the **Let's Encrypt** selection from previous releases.
- In the new ACME Certificates sub-menu, the user can choose *either* Let's Encrypt or DigiCert as an ACME provider. Only one ACME CA can be used per LoadMaster in this release. The ability to use both at the same time will be provided in a future release.
- On upgrade, existing LE accounts and certificates are preserved, and so the DigiCert functionality will not be presented as a choice in the UI -- unless the LE account has been removed. Note that an account can only be removed when there are no more certificates from that vendor installed.
- On downgrade to a release that doesn't support DigiCert account creation for ACME certificate management, any DigiCert certificates that exist at the time of downgrade *will be preserved* in the downgraded system so that VS connectivity is not inadvertently affected by the downgrade. These certificates will be listed on the **SSL Certificates** UI page and can be deleted after the downgrade, if desired.

Virtual Service Sorting

The Virtual Service (VS) View / Manage page has been enhanced to provide sorting of entries in the VS table:

- You can sort by **VIP** (the default), **Name**, **Certificate Installed**, or **Status**. Sorting is performed only on the selected column and is not additive.
- VIPs are sorted with IPv6 followed by IPv4 in ascending order using IP address sorting. Descending sort shows IPv6 followed by IPv4, in descending order.
- Sorting by **Name** in ascending order displays all non-named VSs first, followed by names beginning with special characters, followed by names beginning with alphabetic characters, in ASCII order.
  - In descending order, alphabetic names are displayed first, followed by names beginning with special characters, then non-named VSs.
  - Withing the above groupings (e.g., non-named VSs), entries are sorted by either ascending or descending IP address, as appropriate.
- Sorting by **Certificate Installed** in ascending order sorts all named certificates first in ASCII order, followed by VSs that require certificates but have a default certificate assigned, followed by VSs that do not require certificates (i.e., SSL is disabled).
  - In descending order, it's the reverse: VSs with SSL disabled, followed by VSs that have a default certificate assigned, then VSs with certificates assigned in ASCII order by certificate name.
- Finally, sorting by **Status** in ascending order sorts the VSs in this order:
  - Up (whether checked or unchecked)

- FailMsg
- Redirect
- Sorry
- WAF Misconfigured
- Security Down
- Down
- Disabled

In a descending **Status** sort, the order above is reversed.

Virtual Service Filtering

The Virtual Service (VS) View / Manage page has also been enhanced to provide sorting of entries in the VS table. The currently sorted list can be filtered by the following values using the **Filter By** controls at the top right of the page:

1. Select one of the following:
   - Virtual IP Address,
   - Name
   - Status
2. Then, type the filter text into the text box. The filter is applied as you type.

Clearing the text box removes the current filter.

So, for example: if **Status** is selected in the **Filter By** drop-down and then **Down** is typed into the text box, then only VSs with the status **Down** or **Security Down** will be displayed in the list.

Duplicating a Sub Virtual Service (SubVS)

A new **Duplicate SubVS** button appears at the top right corner of every SubVS. Clicking it will create a new SubVS within the same VS that has the same settings as the SubVS being duplicated except the **Name**, including all Real Servers assigned to the SubVS. The **Name** of the new SubVs is the existing SubVS name appended with an integer.

Chef Template and Deployment Guide

Two new templates and a deployment guide have been created for load balancing requests to the following two **Progress Chef** products:

- **Progress Chef Infra**: allows DevOps teams to define automation policies that are consistent, repeatable, and reusable.
- **Progress Chef Automate**: provides single dashboard and analytics for the infrastructure automation.

One template is provided for each of the above products and is deployed in its own Virtual Service (no

SubVSs). For more information, please see the *Deployment Guide*.

DataDirect Template and Deployment Guide

Two new templates and a deployment guide have been created for load balancing requests to **Progress DataDirect® Hybrid Data Pipeline** configurations, which provide simple, secure, and scalable access to universal data connectivity. One template is provided for SSL offloading on the client side and one for SSL offloading plus server-side re-encryption. For more information, please see the *Deployment Guide*.

License Mobility

Customers can now use a self-service process to transfer their permanent (purchased) license from one LoadMaster to another without assistance from Customer Support. Please note the following:

- It is recommended that customers spin up and configure a LoadMaster with a trial license and then transfer their permanent license to the trial unit.
- The **Kill License** option is used on the currently licensed LoadMaster to return the license to the available pool of licenses. You must supply the license owner's Progress ID (formerly Kemp ID). Once used, *this option will cause the LoadMaster UI to become unresponsive and all services will be interrupted*.
- If the owner of the original license is different from the new owner, you must go through a change of ownership process as well.
- LoadMaster appliance on version 7.2.50 or above is required for this process.
- LoadMaster internet connectivity is required.
- This feature is available for **Online Licensing** only.
- You can only transfer a permanent license for which support has not expired.
- The transferred license can be applied to an existing Trial, Free, or unlicensed LoadMaster.
- The following license types cannot be transferred:
  - Service Provider License Agreement (SPLA)
  - Metered Enterprise Licensing Agreement (MELA)
  - Pooled
  - Pay As You Go (PAYG)

For more details, see this support article and the **Licensing** documentation at this link.

4

Change Notices

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

Related Links

For details, see the following topics:

- GEO: Ignore ECS for Public/Private Decisions
- WAF PCRE Limit Enhancements
- Official Support for VMware 7.0 Update 3d

GEO: Ignore ECS for Public/Private Decisions

Extended DNS (EDNS) Client Subnet (or ECS) is a GEO feature introduced in LMOS 7.2.57.0. This feature leverages a new field in Etended DNS packets that provides a client subnet value set by the client that provide better geographic location of the client compared to earlier versions of DNS without this capability.

Problem: When ECS in 7.2.57.0 is enabled, An incoming request that contains an ECS value always uses the ECS field value (and not the source IP of the request) to determine if a public or private IP should be returned to the client. With the default settings for Public and Private addresses, a private address is returned to the client that is likely not reachable from the client's network.

Example: A client with a private IP address on Site A makes a DNS request to the local DNS server which forwards it to a public DNS server and then on to GEO. If all hops support ECS, then GEO sees the private IP address/subnet in the ECS field and so returns a private IP address. The client, however, will be unable to

reach the expected application using that address.

Solution: The desired behavior is that GEO would instead use the source IP address of the request (which will be the last-hop public DNS server) to determine whether to return a public or private address.

- Change the ECS default behavior so that ECS is ignored and the source IP is checked when the public/private settings are *not* both set to “all sites”.
- Provide a switch (per FQDN) that allows the customer to opt-out of this new default behavior and honor the ECS instead.

The settings and corresponding behavior is summarized in the table below.

ECS Setting	Public & Private Settings	Public / Private Behavior Determined By …	New FQDN Option Effect when Enabled
OFF	Any	Request source IP	When ECS is disabled, the new option is ignored.
ON	!= "all sites"	Request source IP (ECS ignored)	The new FQDN option overrides the behavior at left, so that the request ECS value is used.
ON	!= "all sites"	Request ECS value(source IP ignored)	When the Public & Private settings are both “All Sites”, the new option is ignored.

WAF PCRE Limit Enhancements

To help improve WAF default performance and overall tunability:

- The default PCRE limit has been raised from **1,000** to **10,000**.
- The upper limit on the PCRE value has been extended from **99,999** to **9,999,999**.

The default setting is the recommended initial value but can be tuned if necessary to provide the required depth of WAF analysis. Setting this limit higher than the default should be done only after a determination has been made that a higher WAF engine iteration depth is required for the configuration.

Official Support for VMware 7.0 Update 3d

Release testing has been performed using LMOS 7.2.58.0 to validate official support for **VMware 7.0 Update 3d**. This testing will be performed with each future release.

5

Security Updates

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

Related Links

For details, see the following topics:

- Weak Ciphers Removed from FIPS Cipher Set
- FIPS Mode Cipher Sets Modified to Remove Less Secure Ciphers
- Upgrade: Removed Ciphers in Custom Cipher Sets
- Local User Certificate Login Behavior Switch

Weak Ciphers Removed from FIPS Cipher Set

The FIPS cipher set that is available in normal (i.e., non-FIPS) operating mode has been modified to remove the following three weak ciphers:

- AES128-SHA
- AES256-SHA
- DES-CBC3-SHA

With this change, the FIPS cipher set in normal operating mode contains the same ciphers that are available in FIPS operating mode (see below).

FIPS Mode Cipher Sets Modified to Remove Less Secure Ciphers

In response to changes to US Government standards for FIPS-140-2 certifications, the available ciphers in the LoadMaster certified FIPS product have been modified. [The FIPS certified product is enabled by turning on the **Certificates & Security > Remote Access > Enable Software FIPS Mode** option.]

19 ciphers have been removed from the list of ciphers available in FIPS mode, as shown in the tables below. The remaining 20 ciphers will be the only ciphers available on the system after upgrade.

Supported Ciphers in FIPS Mode	Ciphers Removed from FIPS Mode
AES128-GCM-SHA256	AES128-SHA
AES128-SHA256	AES256-SHA
AES256-GCM-SHA384	DES-CBC3-SHA
AES256-SHA256	DH-DSS-AES128-GCM-SHA256
DHE-DSS-AES128-GCM-SHA256	DH-DSS-AES128-SHA256
DHE-DSS-AES128-SHA256	DH-DSS-AES256-GCM-SHA384
DHE-DSS-AES256-GCM-SHA384	DH-DSS-AES256-SHA256
DHE-DSS-AES256-SHA256	DH-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256	DH-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256	DH-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384	DH-RSA-AES256-SHA256
DHE-RSA-AES256-SHA256	ECDH-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	ECDH-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES128-SHA256	ECDH-ECDSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384	ECDH-ECDSA-AES256-SHA384
ECDHE-ECDSA-AES256-SHA384	ECDH-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256	ECDH-RSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256	ECDH-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384	ECDH-RSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384	

Upgrade: Removed Ciphers in Custom Cipher Sets

Note that, on upgrade from the previous FIPS mode system, any custom cipher sets defined on LoadMaster that include the removed ciphers shown above will remain in those custom cipher sets after the upgrade. You should remove those ciphers from these custom sets to be compliant with the new FIPS cipher guidance either before or after the upgrade.

Local User Certificate Login Behavior Switch

Problem: Customer creates a local LoadMaster user login and also created a Kemp-signed client certificate for that user. They later revoke this certificate using the UI controls, but the user is still allowed to log in using the same certificate.

Explanation: It is the default behavior of the UI that local users with self-signed certificates are allowed to login even after the self-signed certificate expires, as long as that certificate was created by the Loadmaster itself.

Solution: To allow administrators to force LoadMaster self-signed client certificates to expire, a new switch has been provided that enables this checking for local UI logins.

When one of the three levels of client certificate support is enabled for UI login, there is a default minimal level of client certificate checking done in .57 and earlier; the default behavior in .58 (with the new option enabled) is exactly the same.

- The client *must* provide a certificate. The certificate must be either:
  - A match for a certificate chain previously installed on the LM.
  - A Kemp-signed certificate whose SAN/CN field matches a local LM username. [The certificate chain is not validated in this case.]

With the new option *disabled*, LoadMaster will also check certificate chain validity for local user certificates -- and so revocation of a Kemp-signed certificate will now work.

6

Issues Resolved

LM-1817	**Kubernetes Ingress Controller**: Fixed an issue that caused Real Servers to not be added to a SubVS when scaling pods or when creating a new virtual service.
LM-1803	**Kubernetes Ingress Controller**: Fixed an issue that occurred when creating a new namespace -- pods from the default namespace are listed in the output, despite the new name space being the only namespace selected for watching.
LM-1507	**ACME Certificates**: The UI and API limit for the TLD (top level domain) part of an email address was limited to 4 characters. An email address such as “user@domain.**cloud**” would be rejected as invalid. This limit has been increased to 24.
LM-1503	**GEO**: Fixed an issue with high CPU consumption on units with a free license and GEO enabled.
LM-1449	**Content Switching and Client Certificates**: Fixed and issue where enabling content rules caused headers added during client certificate processing to be removed.
LM-1278	**Debug logging**: Fixed a customer-reported issue where log lines were being inappropriately split into two lines, violating the related standard.
LM-1143	**High Availability**: Fixed a customer issue where a failover occurs and (when the configuration is set to anything *except***No Preferred Server**) the two units both attempt to assume the active role, which causes connection loss.
LM-1140	**Logging**: Customers complained of repeated error-level logs of the form “set LOG_LEVEL for 'kernel: L7: Got a bad wkday” message. Since the message cannot be prevented and is common in some configurations, it was changed to a debug level log.

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. This issue has been addressed as described in the following section: Change Notices.
LM-1047	**OCSP Stapling**: In previous releases, no stapled response is sent when an attempt is made to refresh the cache and the OCSP server is not reachable -- it then drops the cached staple. OCSP behavior has been modified to contact the OCSP server to refresh the stapled response; until this refresh is successful, the existing cached staple is not dropped.
LM-1035	**Backup/Restore**: Fixed an issue that causes a backup import to fail when the backup archive contains specific strings.
LM-1001	**LDAP Authentication**: Starting with LMOS 7.2.56, LDAP authentication fails if a user has a Remote User Group configured that is defined in a domain and logs in using a username defined in a sub-domain of that domain. This issue has been fixed.
LM-913	**User Interface**: Fixed a bug in the Intermediate Certificates UI where, when re-encryption is disabled, changes made in the UI are not set.
LM-868	**Admin Login LDAP Authentication Format**: Fixed issues associated with logging in using the domain/username or username-only formats, when groups are also configured.
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 has been addressed and performance levels have been returned to the levels stated in the data sheet.
LM-821	**Kerberos Constrained Delegation (KCD)**: Fixed an issue where a user can login with an invalid domain and password under specific circumstances.
LM-738	**WAF**: Fixed an issue where an error in custom rules could cause the WAF engine to restart.
LM-139	**Backup/Restore**: Fixed an issue where a backup cannot be restored when the file name filename contains specific strings.
LM-81	**WAF**: Fixed an issue where a configuration change under heavy load could cause the WAF engine to restart.
LM-79	**WAF**: Fixed an issue where the WAF engine could restart because of an error in *libapr*.

7

New 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-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-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-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: kernel ssomgr[46119]: segfault at <num> ip <num> sp <num> error 4 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: • Remove and re-add the Virtual Service certificate • 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.

8

Existing 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.
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-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-101	**Statistics**: When upgrading firmware from version 7.1.35.*n*, CPU and network usage graphs are not

59	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.