LOGmanager release notes version 3.2.4

Version:	3.2.4	**Date:**	25th of March 2019

1   Content

2 Introduction

This document describes the following summary of enhancements, support information, installation instructions, list of bug fixes, and description of new features for LOGmanager software version 3.X.X. If you need a detailed description of previous versions of 2.X.X and 1.X.X, see the LOGmanager documentation in the release notes menu or in the LOGmanager user forum here:
https://forum.logmanager.com/viewforum.php?f=4

2.1 Supported models

2.1.1 Version 3.2.2, 3.2.4

The following models are supported:
- LM-36 (2U HP 380 gen8, 12x 3TB HDD, 64GB RAM, 2x6core CPU)
- LM-36B (2U HP 380 gen9, 12x 3TB HDD, 64GB RAM, 2x8core CPU)
- LM-12B (1U HP 360 gen9, 4x 3TB HDD, 64GB RAM, 1x8core CPU)
- LM-DEMO1 (Mini ITX Intel NUC, 1x 500GB SSD, 16GB RAM, 1x2core CPU)
- LM-DEMO-G2 (Mini ITX Intel NUC, 1x 500GB SSD, 32GB RAM, 1x2core CPU)
- LOGM-120TB-D (2U Dell R730xd, 12x 10TB HDD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-D (2U Dell R730xd, 12x 4TB HDD, 64GB RAM, 2x10core CPU)
- LOGM-16TB-D (1U Dell R430, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-H (2U HPE 380 gen9, 12x 10TB HDD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-H (2U HPE 380 gen9, 12x 4TB HDD, 64GB RAM, 2x10core CPU)
- LOGM-16TB-H (1U HPE 360 gen9, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-D-G2 (2U Dell R740xd, 12x 10TB HDD, 3.2TB SSD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-D-G2 (2U Dell R740xd, 12x 4TB HDD, 128GB RAM, 2x10core CPU)
- LOGM-16TB-D-G2 (1U Dell R440, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-H-G2 (2U HPE 380 gen10, 12x 10TB HDD, 3,2TB SSD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-H-G2 (2U HPE 380 gen10, 12x 4TB HDD, 128GB RAM, 2x10core CPU)
- LOGM-16TB-H-G2 (1U HPE 360 gen10, 4x 4TB HDD, 64GB RAM, 1x10core CPU)

2.1.2 Version 3.1.1

The following models are supported:
- LM-36 (2U HP 380 gen8, 12x 3TB HDD, 64GB RAM, 2x6core CPU)
- LM-36B (2U HP 380 gen9, 12x 3TB HDD, 64GB RAM, 2x8core CPU)
- LM-12B (1U HP 360 gen9, 4x 3TB HDD, 64GB RAM, 1x8core CPU)
- LM-DEMO1 (Mini ITX Intel NUC, 1x 500GB SSD, 16GB RAM, 1x2core CPU)
- LOGM-120TB-D (2U Dell R730xd, 12x 10TB HDD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-D (2U Dell R730xd, 12x 4TB HDD, 64GB RAM, 2x10core CPU)
- LOGM-16TB-D (1U Dell R430, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-H (2U HPE 380 gen9, 12x 10TB HDD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-H (2U HPE 380 gen9, 12x 4TB HDD, 64GB RAM, 2x10core CPU)
- LOGM-16TB-H (1U HPE 360 gen9, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-D-G2 (2U Dell R740xd, 12x 10TB HDD, 3.2TB SSD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-D-G2 (2U Dell R740xd, 12x 4TB HDD, 128GB RAM, 2x10core CPU)
- LOGM-16TB-D-G2 (1U Dell R440, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-H-G2 (2U HPE 380 gen10, 12x 10TB HDD, 3,2TB SSD, 128GB RAM, 2x14core CPU)

- LOGM-48TB-H-G2 (2U HPE 380 gen10, 12x 4TB HDD, 128GB RAM, 2x10core CPU)
- LOGM-16TB-H-G2 (1U HPE 360 gen10, 4x 4TB HDD, 64GB RAM, 1x10core CPU)

2.1.3   Version 3.0.1

The following models are supported:
- LM-36 (2U HP 380 gen8, 12x 3TB HDD, 64GB RAM, 2x6core CPU)
- LM-36B (2U HP 380 gen9, 12x 3TB HDD, 64GB RAM, 2x8core CPU)
- LM-12B (1U HP 360 gen9, 4x 3TB HDD, 64GB RAM, 1x8core CPU)
- LM-DEMO1 (Mini ITX Intel NUC, 1x 500GB SSD, 16GB RAM, 1x2core CPU)
- LOGM-120TB-D (2U Dell R730xd, 12x 10TB HDD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-D (2U Dell R730xd, 12x 4TB HDD, 64GB RAM, 2x10core CPU)
- LOGM-48TB-D-G2 (2U Dell R740xd, 12x 4TB HDD, 128GB RAM, 2x10core CPU)
- LOGM-16TB-D (1U Dell R430, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-H (2U HPE 380 gen9, 12x 10TB HDD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-H (2U HPE 380 gen9, 12x 4TB HDD, 64GB RAM, 2x10core CPU)
- LOGM-16TB-H (1U HPE 360 gen9, 4x 4TB HDD, 64GB RAM, 1x10core CPU)

3 Release Notes

3.1.1   Version 3.2.4 - 25 Mar 2019

Improvement of Cluster operation features.
Fixed issues caused by possible "Race Condition" (start of system services in wrong order).

3.1.2   Version 3.2.2 - 5 Dec 2018

Re-design of Cluster operation features/logic.
Added support for a new generation of demo boxes.
If the LOGmanager workload accelerator is present on the system, it is activated and incoming data is primarily processed and stored on NVMe.
Added support for re-importing exported events.
Optimization of embedded parsers.

3.1.3   Version 3.1.1 - 16 Aug 2018

Added support for new generations of HP / Dell servers. All of the current LOGmanager-XL models now include a natively integrated workload accelerator (p/n: LOGmanager-A).

Added support for easy parsing of structured data according to rfc5424.
Added support for data backup.
Many minor upgrades and fixes.

3.1.4   Version 3.0.1 - 30 Apr 2018

Added support for event correlator function (Alerts with thresholds and correlation). Rewritten and actualized blocks.

In the integrated alert templates there are 3 new correlated alert samples:
-   EC Deleted files on file server = detect, if user delete more than 20 files on a file server during context time period.
-   EC 50 bad logins followed by successful login = detect, if user has more than 50 failed logon attempts followed by successful login. In other words, detection of successful dictionary attack.
-   EC too many failed logins = detect, if user has more than 5 failed logons.

All integrated alert samples can be modified and based on those samples, You can create new alerts with thresholds or correlation. **Important notice**: All messages passing through the alerts with context require up to 4 times more processing time. Therefore, it is not a best practice, to count in alert with context for example -> how many times each source IP address communicate through firewall. For such queries, please use dashboard functions.

LOGmanager version 3.0.1 consists of many changes and it is not possible to downgrade it to the former version without backup/restore! We recommend to backup configuration before the upgrade.

4 New Functions

4.1.1 Version 3.2.4

- No new functions in this release.

4.1.2 Version 3.2.2

- Re-design of Cluster operation features/logic. Please, find the detailed description of new cluster function in LOGmanager documentation here: link.
- Added support for re-importing exported events.
    - o LM will download the backup from an external SMB server and import it back to the system.
    - o All re-imported data is marked.
    - o Imported data is not automatically deleted from the system, it must be manually deleted from the Database status page.
    - o Currently, only one simultaneous import is supported; for importing multiple days, it is necessary to wait for the task to finish, before entering another import.
- Added support for the built-in LOGmanager workload accelerator in the new generation of LM boxes. If present, LM will automatically create two database instances, one instance on the HDD and one instance on NVMe. All incoming data is indexed to NVMe, after optimization, the data is automatically moved to the HDD.
- The parsing engine now uses runtime optimization for all built-in parsers. Internal parsers after this optimization need 20-50% less CPU for parsing operations.
- The Cluster newly performs periodic cluster integrity checks (sequentially opens, checks, and then closes historical data). Originally, this was done only when the system was started, and this feature is newly spread over time.
- Added new internal monitoring, in next versions will be consequently made available in dashboards. (ie. graphs of load, number of messages, etc.)
- Added an endpoint API to create a support package on request. The package contains diagnostic command outputs, internal application logs, and partial configuration (the package does not contain any sensitive data = user passwords / AD / components or SSL certificates).
- Optimization of the internal queue run, double acceleration of the input for parser engine.
- Optimizing automatic opening and closing of historical data. Data searches over 8 days were accelerated by 5-30 seconds.
- SQL Component - added support for collecting events in tables that use datetime2 format.
- Added a Squid (proxy) dashboard.

4.1.3 Version 3.1.1

- Revised Database status view page. It newly displays status of all daily indexes, which are stored in LM, and allows manual opening and closing indexes for individual days.
    - o Dashboards continue to automatically look after opening indexes and automatically close the index again after searching the data. Data search does not require to manually open indexes.
    - o Each database search action creates new database locks. Locks are created for both system and user queries. If there is a lock on the index, the index cannot be closed. Open locks will automatically close after 4 hours.
    - o The system does not allow to open and search more data, than is the capacity of available system memory.
    - o Added possibility to export selected daily index to external SMB server.
- Added support for collecting and parsing logs in a structured format according to rfc5424.
- The parser test window now supports embedding of the entire syslog message without having to trim the raw_offset. The offset is now calculated automatically, and it is possible to work with a standard syslog header (programname, etc.).
- Added support for archiving data on an external SMB repository. According to settings, system will each day backup collected logs to a defined SMB server. Backup data is compressed using GZip algorithm.
- Change of the LOGmanager hostname. Old hostname was "LOGmanager", now the hostname is a serial number of the LOGmanager to simplify distinction between cluster members.

4.1.4 Version 3.0.1

- Added event correlator (Alert with Thresholds and Alert with Correlation rules).
    - o Added Alert Contexts lifetime definition within range 60 to 900 seconds.
    - o Added new templates for Alerts with Thresholds and Alert with Correlations.
- Parsers and alerts newly enable the use of mathematical operations.
- Parsers and alerts newly support URL decoding (scheme, netloc, path, params, query, fragment, hostname, username).
- Added block which enables discarding of the received message.
- Added support for multicolumn lookup tables.
- Removed function of adding town name to IP addresses, high inaccuracy for individual addresses (reason: more than 90% towns were assigned with very low accuracy).
- Added support for a new generation of Dell servers (-G2).
- Increased number of parsing processes by 40%.
- Added button for deactivating of automatic translating of DNS PTR records at IP addresses. In case of logging large part of firewall traffic, significant slowdown of parsing processes happened because of DNS slowdown and waiting for responses. In extreme cases of logging IP addresses with non-existent/non-responding DNS servers, up to 90% slowdown of parsing processes happens.
- Checkpoint – update of OPSEC SDK.
- Checkpoint – added internal ping within the OPSEC protocol for communication status control within the OPSEC tunnel.

5   New parsers:

5.1.1   Version 3.2.4
- New parsers:
    - o   Safetica DLP
    - o   Synology DSM
- Updated parsers:
    - o   Microsoft Windows - fixed wrong tags assignment for EventID: 4776 with status: 0x0
    - o   Mikrotik - added support for DHCP and forward logs

5.1.2   Version 3.2.2
- New parsers:
    - o   Symantec Endpoint Protection Manager
    - o   Symantec Messaging Gateway
    - o   Squid
    - o   Junipersrx structured data log
    - o   Junipersrx-lite
    - o   Barracuda Email Security Gateway
- Updated parsers:
    - o   Microsoft Sharepoint
    - o   Windows-firewall - completely re-written, performance optimized
    - o   HPE - Comware OS
    - o   Squid - added support for logs from windows environment
    - o   Huawei USG
    - o   Windows
    - o   Unifi
    - o   Cisco IOS
    - o   Cisco ASA
    - o   Normalization of all email addresses across all parsers
    - o   Palo Alto

- Across all parsers, email addresses are now normalized to same format.

5.1.3   Version 3.1.1
- New parsers:
    - o   FortiManager
- All integrated parsers revised and updated. Improved and optimized work with message parsing. In the next version of LM, there will be added features accelerating parsing of all the integrated parsers by 20-50%.

5.1.4   Version 3.0.1
- New parsers:
    - o   FortiGate-lite
        - ▪   light version of the parser, which parses only selected fields.
        - ▪   Parser is about 30% faster than standard fortigate parser.

- Selected fields: app, appcat, count, device_id, device_name, dst_iface, dst_ip, dst_port, duration, logdesc, msg, policy_id, protocol, rcvd_byte, rcvd_pkt, reason, sent_byte, sent_pkt, service, src_iface, src_ip, src_port, status, subtype, type, username, vd, vpn.
  - Cisco Nexus
  - Huawei USG
  - Palo Alto
  - Extreme NAC
  - Ruckuss wireless
- Updated parsers:
  - HP Comware
  - FortiGate
    - Parser newly doesn't parses other duplicit or unnecessary fields (crscore, craction, lanin, lanout, logtime, app_id, attack_id, cat, icmpcode, icmpid, icmptype , log_id, mastersrcmac, port, reqtype, sessionid, vip, wanin, wanout, wanoptapptype, countapp, countav, countweb, method, profiletype, ref, sslexempt).
  - ISC DHCP
  - Windows DHCP
  - Windows
  - Freeradius
  - Aruba
  - Checkpoint – parser newly parses also the logs received via syslog (BSD format)
  - Trapeze
  - LOGmanager
  - Kaspersky - parser newly parses also the logs received in CEF format
  - FortiMail
  - JuniperSRX
  - Cisco SMB
  - Cisco IOS

6   Corrected errors

6.1.1   Version 3.2.4
- Version 3.2.2 did not make stored data available when the master server was lost and the cluster was manually disconnected.
- When connecting boxes to a cluster, all data on the "slave" box is erased when cluster is created.
- Race condition, fixed possible situation, where the premature activation of the Workload Accelerator could cause the old indexes to be copied to the Workload Accelerator, fully utilizing its storage. The new incoming data was still processed correctly, but after this Race Condition, it was stored on the HDD directly instead of processing on the Workload Accelerator. This Race condition cause no data loss.
- Race condition, the internal process of database could end up with a database error when a specific combination of circumstances occurred. Newly incoming data was buffered and data loss could occur after 50GB buffer was exhausted.

6.1.2   Version 3.2.2
- Fixed SMB protocol error in LM, where old SMB protocol was used by default. Now works with SMB2 and SMB3 by default.
- Fixed an error, when it was necessary to manually restart the slave box after joining LM to the cluster. The slave box will now automatically reboot when you connect it to the cluster.
- Fixed SSL/RELP certification changes error.
- Fixed an error, when it was possible for a user to create a loop in the certificate chain.
- Fixed display of the database group description.
- Fixed display of data in dashboards (if topN events were searched for more than a few days, it could display the error message instead of the expected result).
- Fixed incorrect postfix hostname.
- Fixed an error when backup configuration could not be changed, if SMB server was unavailable.
- Fixed the Database status view for Edge.
- Removed excessive user rights to edit LDAP groups for non-admin group users.

6.1.3   Version 3.1.1
- Fixed dashboard search error, that could rarely lead to system database crash. It was possible to see such condition on very busy systems during search over an excessive (30+ days) period of time.
- Fixed Linux kernel security vulnerability CVE-2018-5390.
- Removed HTTP HSTS header for Strict-transport-security. Such header was forbidding the browser to connect to a webserver with expired HTTPS certificate. If the certificate had been expired, by using HTTP HSTS header, it was not possible to change or restore the certificate.
- Fixed traceroute command in CLI.
- Fixed security vulnerability of dashboards. This bug allowed the dashboard environment to run the JS code, scammed into the received syslog message. HTML characters seen in the messages are now fully escaped.
- Fixed a parsing process error when the parser regular expression was broken. An error message about a wrongly created regex is now displayed.

- Fixed rare alert test window error. Now the test window alert condition information is always correctly displayed.
- The VMware component now correctly adds tags.

6.1.4 Version 3.0.1
- Update of the Linux kernel to the version with integrated protection against Meltdown/Spectre attacks. It is not and has never been possible to attack LOGmanager with any of these attacks. Detailed Security Advisory can on LOGmanager user forum.
- In certain cases, malfunction of adding tags to windows agents.
- Improved internal logging of the syslog forwarder (connection timeout, connection reset).
- Various fixes of minor issues with parsing process, added warnings of possible error states during message processing.
- Event export to external syslog did not work at highly loaded box.
- Permission adjustment for Windows agent download, now it can be downloaded by anybody with permission for Windows section.
- SQL – Repaired malfunctioning connection to Microsoft SQL server instance.
- SQL – Repaired error of when incorrectly connected, the SQL agent logged thousands of errors.
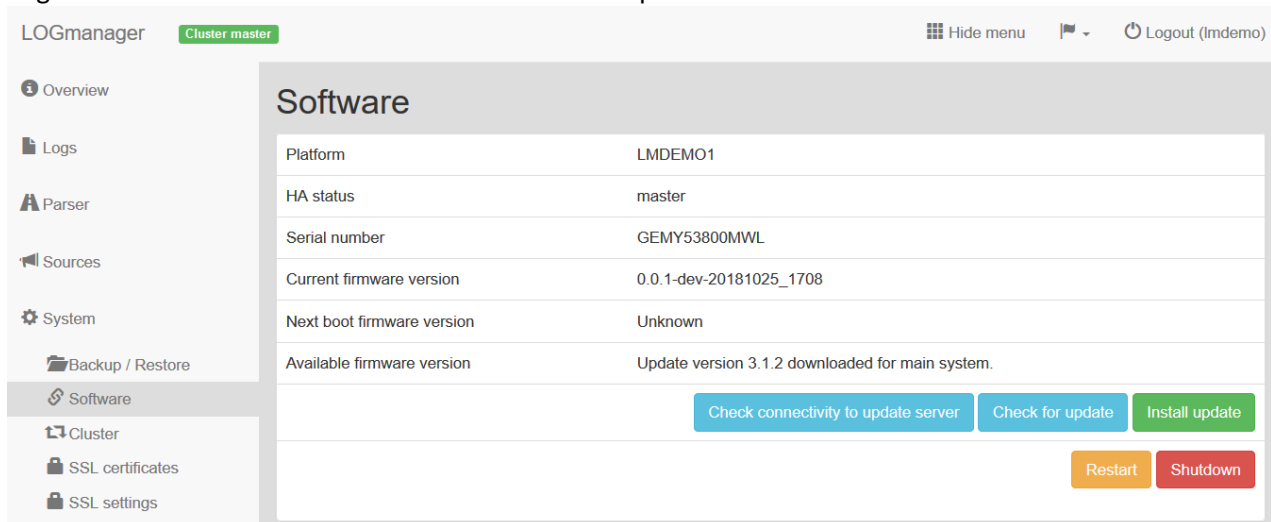
7 Known bugs

7.1.1 Version 3.2.2, 3.2.4
- Problem:
  - Configuration screen containing Blockly sometimes does not load the blocks properly. Issue could appear mostly while using Chrome web browser.
- Workaround:
  - Reload the page.

- Problem:
  - Configuration screen containing Blockly sometimes does not show translated tag names (IDs of the tags are displayed instead of tag names)
- Workaround:
  - Switch to XML view and back, tags will be translated correctly.

- Problem:
  - After upgrade to LOGmanager software 3.1.1 - in menu Overview / Database status, older daily indexes show zero size.
- Workaround:
  - LOGmanager, after the upgrade, does not know exact size of the daily indexes, which had not been open yet. Open the index manually, or search through given date in dashboard and the correct size of the index will appear.

8 Update process

WARNING: Release 3.2.4 DOES NOT SUPPORT gradual cluster upgrades. You need to upgrade the cluster by installing a new SW on both boxes and restarting both cluster nodes at the same time.

For new version installation in WEB interface click on System > Software
Page with information about installed software will open

Upgrade process:
- Click the button "Check for update".
- Available Version **3.2.4** will be displayed.
- Click the button "Install update".
- Once the page is reloaded, in **next boot firmware** will be displayed **3.2.4.**
- In the last step, just click Restart and system will restart to the new Version.

8.1.1   After server restart

After restarting the server, it is necessary to delete the browser cache for the proper functioning of the web interface!

After each update, the database integrity check is performed. After the server restart, the status of the database is always in the red state and the check is performing, this is normal status after the upgrade - after the check is complete, the status returns to normal state.
No new data is stored in dB for the duration of the integrity check! However, the received events remain in the internal cache and are inserted into the dB as soon as the check is complete. The scan may take up to 30 minutes depending on the size and number of stored events.

End of document.