LOGmanager release notes version 3.6.1

Version:	3.6.1	**Date:**	9th December 2020

1 Content

LOGmanager release notes version 3.6.1 1
2 Introduction 3
2.1 Supported models 3
2.1.1 Versions 3.5.2 - 3.6.1 3
2.1.2 Versions 3.3.0 - 3.5.0 3
2.1.3 Version 3.2.2, 3.2.4 4
2.1.4 Version 3.1.1 4
2.1.5 Version 3.0.1 5
3 Release Notes 6
3.1.1 Version 3.6.1 6
3.1.2 Version 3.5.2 6
3.1.3 Version 3.5.0 6
3.1.4 Version 3.4.0 6
3.1.5 Version 3.3.0 7
3.1.6 Version 3.2.4 7
3.1.7 Version 3.2.2 7
3.1.8 Version 3.1.1 7
3.1.9 Version 3.0.1 7
4 New Functions 9
4.1.1 Version 3.6.1 9
4.1.2 Version 3.5.0 10
4.1.3 Version 3.4.0 11
4.1.4 Version 3.3.0 11
4.1.5 Version 3.2.4 12
4.1.6 Version 3.2.2 12
4.1.7 Version 3.1.1 13
4.1.8 Version 3.0.1 13
5 New parsers: 14
5.1.1 Version 3.6.1 14
5.1.2 Version 3.5.0 14
5.1.3 Version 3.4.0 14
5.1.4 Version 3.3.0 14
5.1.5 Version 3.2.4 15
5.1.6 Version 3.2.2 15
5.1.7 Version 3.1.1 16
5.1.8 Version 3.0.1 16
6 Corrected errors 17
6.1.1 Version 3.6.1 17
6.1.2 Version 3.5.2 17
6.1.3 Version 3.5.0 17
6.1.4 Version 3.4.0 17
6.1.5 Version 3.3.0 17
6.1.6 Version 3.2.4 18
6.1.7 Version 3.2.2 18
6.1.8 Version 3.1.1 19
6.1.9 Version 3.0.1 19
7 Known bugs 20
7.1.1 Versions 3.3.0 - 3.6.1 20
8 Update process 21
8.1.1 After server restart 21

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 Versions 3.5.2 - 3.6.1

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)
- 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)
- LOGM-8TB-D (Tower Dell T140, 2x 4TB HDD, 32GB RAM, 1x2core CPU)
- LOGM-48TB-H-G3 (2U HPE 380 gen10, 12x 4TB HDD, 128GB RAM, 2x12core CPU)
- LOGM-16TB-H-G3 (1U HPE 360 gen10, 4x 4TB HDD, 64GB RAM, 1x12core CPU)
- LOGM-48TB-D-G3 (2U Dell R740xd, 12x 4TB HDD, 128GB RAM, 2x12core CPU)
- LOGM-16TB-D-G3 (1U Dell R440, 4x 4TB HDD, 64GB RAM, 1x12core CPU)
- LOGM-144TB-D-G3 (2U Dell R740xd, 12x 12TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-144TB-H-G3 (2U HPE 380 gen 10, 12x 12TB HDD, 128GB RAM, 2x16core CPU)

2.1.2 Versions 3.3.0 - 3.5.0

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)
- LOGM-8TB-D (Tower Dell T140, 2x 4TB HDD, 32GB RAM, 1x2core CPU)
- LOGM-48TB-H-G3 (2U HPE 380 gen10, 12x 4TB HDD, 128GB RAM, 2x12core CPU)
- LOGM-16TB-H-G3 (1U HPE 360 gen10, 4x 4TB HDD, 64GB RAM, 1x12core CPU)
- LOGM-48TB-D-G3 (2U Dell R740xd, 12x 4TB HDD, 128GB RAM, 2x12core CPU)
- LOGM-16TB-D-G3 (1U Dell R440, 4x 4TB HDD, 64GB RAM, 1x12core CPU)

2.1.3 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)

2.1.4 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)

2.1.5 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 3.6.1

CAUTION - This release contains a notice about the planned termination of support for the CheckPoint component for getting CheckPoint logs via the OPSEC protocol. For information on how to set up CheckPoint Firewalls to use the CheckPoint log export instead, see our documentation. We kindly ask customers who use CheckPoint to collect logs via the settings in the Resources / CheckPoint menu, to change their configuration till the next version of the LOGmanager software.

Lightweight parsers. It is now possible to easily enable "Lite" parsers without having to modify the data classification. For loaded boxes (CPU utilization constantly over 70%), it is advisable to start using these lightweight parsers. This is because they generate fewer fields during data processing, which reduces CPU, disk array and system memory utilization.

Test window (known from parsers and alerts) now also in the classification of input data.
The IP address field now contains a sub-field with the number and name of the AS (autonomous system).
Digital signing of backups.
Enhancements to the Role-Base Access Control (RBAC) feature to increase the number of concurrent system operators.
Optimization of work of internal balancing queues.
Optimization and acceleration of data processing in the cluster - increase of performance by 30-40% and data replication by 75%.
6 new and 9 modified parsers, 6 new dashboards.
Added complete support for new generations of servers (G3).
Other minor fixes and improvements.

3.1.2 Version 3.5.2

CAUTION - This release contains version 3.5.0 bug fixes. If you are using version 3.5.0, we recommend that you update as soon as possible!

This release fixes a bug that could, under certain rare circumstances, cause system-wide services to crash.

3.1.3 Version 3.5.0

Caution - a significant change in the behavior of classifiers.
The upgrade simplifies the classification parameters. For more details, see the detailed description of new features in this release notes section 4.1.1.

Attention - possible upgrade of Dell PERC firmware
The upgrade automatically detects and updates the Dell PowerEdge Raid Controller firmware on LOGmanager models, where needed.

Improvements to VMWARE and SQL components.
New blockly block.
WES (LOGmanager Windows Event Sender) now uses the cryptographic protocol TLS 1.2.
New dashboards and alert templates
Minor fixes and improvements.

3.1.4 Version 3.4.0

Correlations and Alerts with Thresholds - Maximum context time increased from 15 to 30 minutes.
Added possibility to reduce DNS PTR only to a given IP prefix list.
New blockly blocks.

Minor bug fixes and enhancements.

3.1.5 Version 3.3.0

Added support for Office365.
Added support for Syslog over TLS.
Added support for authentication and encryption of SMTP.
Added support for NXLOG Windows agent.
Enhanced support for integration with 3rd party SIEM/UBA.
Minor bug fixes and enhancements.

Changed behavior of reading data from Oracle databases.
After update to 3.3.0 version and it's components (components should automatically update after reboot to new version under 30 minutes) please check if reading from Oracle database is functional. We fixed behavior of reading data from Oracle by standard. If you read data using synonym, you must enter synonym name to table field with UPPER CASE letters (as stated in documentation for synonyms in Oracle database).

Added basic product telemetry.
Beginning with this version of the software, the device features & usage statistics is added and turned on by default. The data sent is as anonymous as possible. Telemetry do not contain any sensitive data or specific data, only information about what LOGmanager functions are used and in what quantity. This feature can be turned off in the LOGmanager menu: Users > Authentication. There is also a preview of the data that is sent via this basic telemetry to the manufacturer. LOGmanager does not send any information for the first 7 days after upgrading to this version. If possible, leave statistics sharing with the manufacturer turned on. This will allow the LOGmanager development team to better track which features to focus on with further development of the product.

3.1.6 Version 3.2.4

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

3.1.7 Version 3.2.2

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.

3.1.8 Version 3.1.1

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.

3.1.9 Version 3.0.1

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 3.6.1

- Caution: Log reading from CheckPoint using component / LEA protocol has been marked as EOL and will be obsoleted in the next version of LOGmanager software. CheckPoint logs can now be preferably sent using Syslog or Syslog via TLS, according to the instructions in the LM docs.
- Added test message window to classifiers. Note: In this version of the code, the window verifies the classification method only against the block in the given classification window / classification template.
- Added another set of so-called lite parsers, which parse only the most important information. Settings for how the data will be parsed can now be made in the Lite-parser-Settings lookup table. The use of the lite parser can speed up the system and significantly reduce the size of daily indexes, especially for windows logs. (Example for Windows logs - efficiency of using the "microsoft-windows-lite" parsing rule: 50% smaller size of daily indexes, 75% less memory consumption and 20% faster indexing.)
- Reduced the time of the system script, which takes care of data replication within the cluster. Originally opening and closing old indexes every hour, it now performs this operation every 15 minutes. This change will significantly speed up the synchronization of new clusters.
- Added ip2asn functionality, AS number (autonomous system) + AS name is newly added to all IP addresses, for greater efficiency of security analyzes and statistics.
- Added the function of automatic digital signing of exported database backups. Using 4096bit certificates generated in LM at system startup, each backup file is now automatically signed and signature can be evaluated externally or during the restore procedure. (complete description in the documentation).
- Reduced the number of automatically open daily indexes from 8 to 6. This change brings performance improvements and the ability to search a larger amount of historical data on heavily used LM.
- Improved cluster indexing performance by 30 to 40% over a stand-alone unit. The individual nodes in the cluster now automatically distribute the indexing load.
- Significant optimization of the internal queue system, newly optimized queues need about 10 times less IO operations for their operation. This enhancement greatly improves device performance as it queues.
- Newly, all modified or newly created parsing rules will contain in the description information about the last update date and the tested software version of the source system for which the rule is written.
- Added a new RBAC privilege on system groups (search / read-only), which allows a user with a given system group to search only the data of currently open indexes. Suitable for operators who do not need or do not have to see the historical data of the system.
- Added complete support for new generation servers. LOGmanager SKU ends at G3.
- New and modified dashboards:
    - Dell iDrac
    - Synology NAS
    - Veeam
    - VMware status change
    - VMware user session

- VMware overview
- CEF Flowmon
- FortiGate traffic log
- Windows update

4.1.2 Version 3.5.0

- Caution: Significant change in the behavior of classifiers. The data source for the classification had been removed globally. The result of the modification is the unification of rules. Since LOGmanager version 3.5.0 on, it is possible to sort data from all sources by using one classification. Compatibility with previous user modification of the classifiers is maintained.
  - This change will significantly simplify the classification and tagging of data.
  - Renaming predefined classifiers to “vendor-*” clearly distinguish classifiers created by the manufacturer from newly / user-created classifiers.
  - Simplification of predefined classifiers and additional resources for optimal functionality.
  - All new LOGmanagers with version 3.5.0 and above will contain just one default classifier named as vendor-default. It sends all the data to classifier template vendor-default-classification for processing of all sources.
- Caution: Dell PERC H470P controller contain error up to version 50.5.1-2633:
  - The controller firmware contains an error that can cause data loss when replacing a damaged disk.
  - LOGmanager will automatically perform a complete RAID check, upgrade the controller firmware, and then perform a second data integrity check. LOGmanager automatically notifies the administrator of the need to restart the server to apply the new firmware version to the controller = **please check the SMTP settings!**
  - Both checks and automatic upgrades are run with low priority, expect a significant delay before LOGmanager send email notification with a restart request.
- VMware component:
  - Update for proper functionality with VMware 7.x.
  - Improved component logging.
- SQL component:
  - Added support for reading exact time for Oracle databases.
  - Improved error logging and timeout operations.
- NTP improvements. Overview / System status screen now shows the current status of the NTP process and time synchronization.
- New automated notification of a problem with automatic database backup had been added. If a problem with automatic database backup is detected, the LOGmanager administrator is now informed by email.
- New blockly text block "decamelize" – Sample: converts the text "SomeValueA" to "some_value_a".
- WES agent now uses TLS 1.2. After the first connection to the LM server, the Windows agent will automatically start using TLS 1.2 instead of the original TLS 1.0, which MS dotnet automatically prefers.

- New and improved dashboards:
  - Windows updates
  - O365 overview
  - O365 Azure AD

- O365 Exchange
- O365 Exchange DLP/transport log
- O365 OneDrive
- O365 Power BI
- O365 SharePoint
- O365 Teams
- Webservers access log
- New account overview
- Sharepoint
- Linux Bash Activity

Note: Where is necessary to perform additional configuration on the source system to obtain data for LOGmanager use-cases, the dashboards now contain a minimized field with a step by step source config guide.

- New alerts and templates:
  - New-account
  - Linux-bash-activity
  - O365-new-user-added
  - O365-user-added-to-admin-role
  - O365-user-login-from-unusual-region
  - Webserver-excessive-number-of-404-error-codes
  - Windows-update-failure

4.1.3 Version 3.4.0

- Unique event ID in every message in field "meta.event@id".
- Correlation templates now contain tracing of "event@id" that took part in correlation.
- Alerts and classifiers - restrictions of blocks available for operations is now removed.
- New blockly block "in text replace" added.
- New option in blocks "raw_real" is available. This variable contains full message without stripping by "raw_offset". Use for processing messages that do not follow standard syslog header.
- Added possibility to reduce DNS PTR only to a given IP prefix list. System-wide DNS PTR can significantly reduce performance in certain deployments. Defining address space for DNS PTR brings balance between performance penalty and desired functionality. By default, the DNS PTR is enabled for all IPv4 and IPv6 addresses.
- Classifier and classifier templates overview enhanced and simplified.
- Correlations and Alerts with Thresholds - maximum context time increased from 15 to 30 minutes.
- Parsing processes (IP prefix list lookup and Regex cache) optimized for performance.
- New dashboard for Office365.

4.1.4 Version 3.3.0

- Telemetry - Sending statistics on usage of LOGmanager functions to the manufacturer. What is being sent can be displayed and optionally disabled in LOGmanager menu Users> Authentication.

The device will not send any data for the first week after system startup or upgrade. Please leave this feature enabled, if possible.

- Added support for Office365. Obtaining logs from Microsoft cloud environment.
- Added support for SMTP authentication and encryption of SMTP server connections.
- Added support for receiving logs from NXLOG Windows agent, LOGmanager treats these logs as if they were received from LOGmanager native Windows agent (adding tags, auto-expanding JSON in classifiers, etc.).
- Added missing blocks to Alerts - all sections of data processing now contain the same blocks.
- Added support for receiving logs using Syslog over TLS.
- Added alerts when building a cluster with warning information that all data on the "slave" system will be deleted.
- Added custom description field to tags.
- Syslog output now allows to set 4 different forwarded message formats. This option provides easier integration with third-party SIEM / UBA systems. (IBM QRadar, etc.).

4.1.5 Version 3.2.4

- No new functions in this release.

4.1.6 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.
    - LM will download the backup from an external SMB server and import it back to the system.
    - All re-imported data is marked.
    - Imported data is not automatically deleted from the system, it must be manually deleted from the Database status page.
    - 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.

4.1.7 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.
    - 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.
    - 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.
    - The system does not allow to open and search more data, than is the capacity of available system memory.
    - 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.

4.1.8 Version 3.0.1

- Added event correlator (Alert with Thresholds and Alert with Correlation rules).
    - Added Alert Contexts lifetime definition within range 60 to 900 seconds.
    - 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 3.6.1

- New parsers:
  - Windows lite
  - Cisco ASA lite
  - Veeam Backup & Replication
  - Hillstone NGFW
  - Microsoft Exchange tracking log
  - Pulse Secure
- Updated parsers:
  - Huawei – added new formats
  - Postfix – improved parsing
  - Checkpoint – added new formats
  - LOGmanager – improved internal message parsing
  - Windows DHCP – added lookup table
  - HP Aruba – improved parsing
  - Flowmon – now with severity # to text translation, additional msg.msg field content parsing
  - Firepower – improved parsing and optimization
  - Windows – improved parsing and optimization

5.1.2 Version 3.5.0

- New parsers:
  - Oracle audit db
  - Windows DNS debug log
  - AIP-safe
  - Bash
- Updated parsers:
  - Fortimail – support for latest release of Fortimail OS
  - O365 – improved parsing
  - Windows – improved parsing
  - Tomcat – added support for Tomcat on Windows platform

5.1.3 Version 3.4.0

- Updated parsers:
  - Windows – fixed wrong tags assignment for EventID: 4776 with status: 0x0
  - PaloAlto – Support for BSD message format
  - ArubaOS – Support for CEF message format introduced in Aruba 8.x
  - Optimized parsing in those parsers: Huawei, Sophos, Juniper, Exchange, epacs, Checkpoint, Greycortex, PaloAlto, Aruba

5.1.4 Version 3.3.0

- New parsers:
  - Greycortex
  - Radware Defens Pro

    - F5 ASM
    - Cisco ISE
    - Cisco UCS
    - Office365
    - ePacs
- Updated parsers:
    - Safetica DLP
    - Synology DSM – Structured logs based on RFC5424
    - Windows – updated translation tables, enhancing tags
    - Squid
    - Mikrotik
    - Cisco-ASA - support for Firepower logs
    - HP-Aruba
    - HP iLO
    - Flowmon
    - Palo Alto
    - Checkpoint
    - SSH

5.1.5 Version 3.2.4

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

5.1.6 Version 3.2.2

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

- Palo Alto

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

5.1.7 Version 3.1.1

- New parsers:
  - 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%.

5.1.8 Version 3.0.1

- New parsers:
  - 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 3.6.1

- Updated kernel - fixes very slow communication with the disk controller on some HP servers.
- Fixed LEEF decode block, which can now decode according to the complete specification of LEEF format.
- Fixed backup export to external SMB server, under certain conditions incomplete backup could be copied on heavily loaded systems. Improved backup logic and efficiency.
- Improved display of NTP status page by other possible statuses of NTP service.
- Temporarily removed trunk (link aggregation) interface configuration from CLI LM.
- Events processed by the user parser, which did not have a return block in them, were not sent for further processing in alerts. It caused confusions. Newly, all traffic is sent for processing in alerts.
- Fixed memory leak bug in processes taking care of DB running, exports, closing / opening indexes, etc. The bug caused processes to consume more memory than designed. The result could be a slowdown of the whole system.

6.1.2 Version 3.5.2

- Fixed a possible crash of the services of the entire LOGmanager system. We managed to replicate this state only on LMDemo boxes, but as a precaution, we issue a fix for all LOGmanager models.
- Fixed LEEFv2 decoder.
- SQL component fix - under certain circumstances, reading from tables using a timestamp in "datetime" format might been suspended. ("datetime2" format is no problem)

6.1.3 Version 3.5.0

- Alert did not send an email notification in case of incorrectly defined formatting template. New information about the wrong configuration and the event causing this, is sent by email.
- The newly used NTP Chrony enables more stable synchronization with native (not exact) NTP implementations of Microsoft server operating systems.

6.1.4 Version 3.4.0

- Syslog output could under certain combination of non-ASCII characters in message refuse to forward such message.
- WEB-API now provides detailed description of discovered error conditions.
- Fixed sorting of Windows agents by date/time of last connection.
- Removed blockly block "foreach" in conjunction with IP prefix lists. IP prefix list can be queried only by block "if in", as described in documentation.
- Fixed Juniper dashboard and several alert templates.

6.1.5 Version 3.3.0

- Fixed "race condition" error where system boot might start under certain circumstances before disc subsystem is fully available.
- Fixed bug with not displaying IP addresses on LOGmanager console, which occurred with certain IP address settings.

- Fixed wrong escaping of Unicode regular expressions in Parsers. It is now possible to use any Unicode characters inside Regex.
- Fixed SQL connector - under certain conditions it did not respect configuration changes in the GUI and was still running with the previous configuration.
- Fixed SQL connector in some configuration it refused to connect to Oracle database. We modified internal behavior of component. **If you data from synonym instead of SQL table, you must now enter synonym name in UPPER CASE format as Oracle states in it's documentation.**
- The SQL connector may not have correctly read the logs from the MSSQL server due to poor transaction termination.
- Fixed dashboard documentation links.
- Improved Regex substitution for MAC address detection and normalization.
- Fixed SMTP configuration bug that may allow notifications to be sent through other than SMTP server defined in configuration.
- Fixed VMWare connector error when it could stop reading logs in certain circumstances.
- Report generation has been fixed. If a large number of reports were generated in a short period of time, some reports could be sent without populating data.

6.1.6 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.

6.1.7 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.

6.1.8 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.

6.1.9 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 Versions 3.3.0 - 3.6.1

- 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.

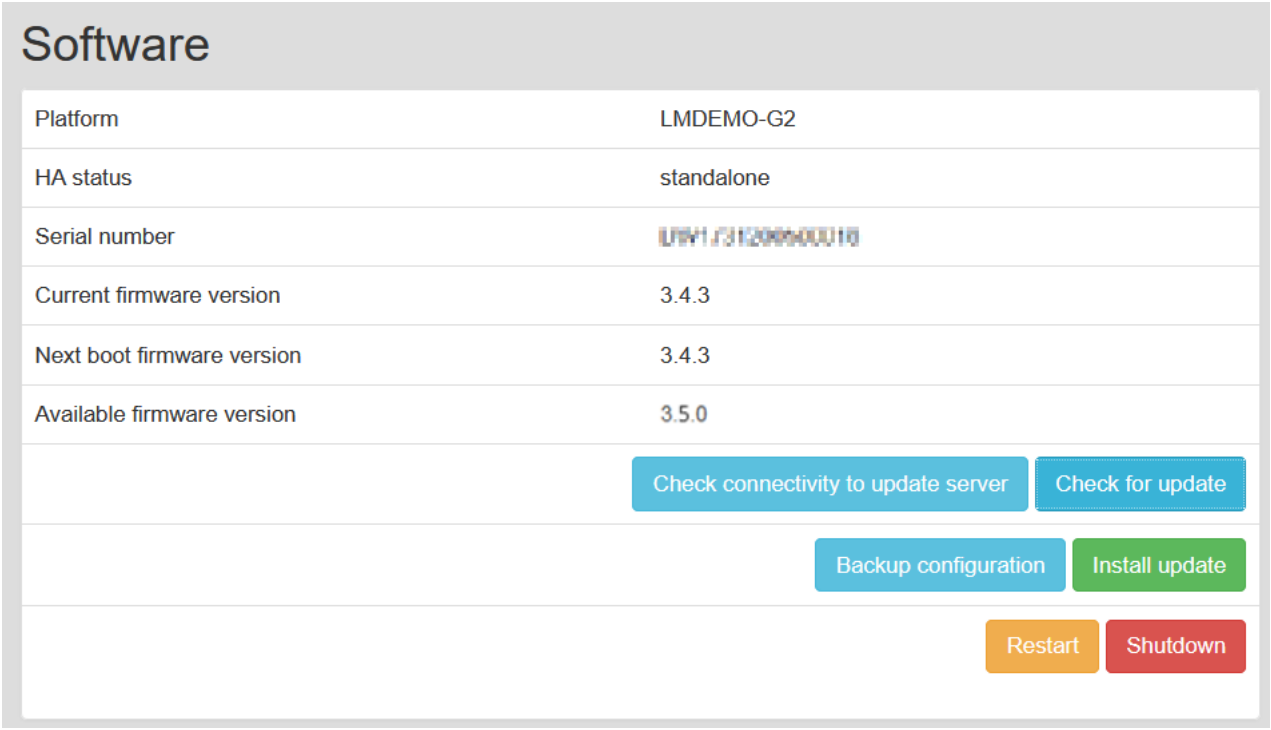
- Problem:
  - Configuration screen containing Blockly sometimes does not show translated tag names (IDs of the tags are displayed instead of tag names)
- Workaround:
  - Switch to XML view and back, tags will be translated correctly.

- Problem:
  - While editing Blockly (in classifiers, parsers, alert) block “add tag” with creation of new tag name, sometimes it is not possible to save the edited work (with red error notification strip).
- Workaround:
  - You cannot create new tag with the name already present in the system. Change the tag name to something else. Now, the save is not reporting the error.

8 Update process

WARNING: Release 3.6.1 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 **3.6.1** will be displayed.
- Click the button “Backup configuration” to backup the config prior upgrade.
- Click the button “Install update”.
- Once the page is reloaded, in **next boot firmware** will be displayed 3.6.1**.**
- 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.