LOGmanager release notes verze 3.5.0

Verze:	3.5.0	**Datum:**	05.06.2020

1 Obsah

2 Úvod

Tento dokument popisuje následující souhrn vylepšení, informace k podpoře, instalační instrukce, seznam opravených chyb a popis nových funkcí pro verze kódu 3.X.X. Pokud potřebujete podrobný popis pro předchozí verze kódu 2.X.X a 1.X.X, naleznete jej v dokumentaci LOGmanager v menu release notes nebo na uživatelském fóru LOGmanager zde: https://forum.logmanager.cz/viewforum.php?f=4

2.1 Podporované modely

2.1.1 Verze 3.3.0, 3.4.0, 3.5.0 - Podpora následujících modelů:

- 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)

2.1.2 Verze 3.2.2, 3.2.4 - Podpora následujících modelů:

- 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)

2.1.3 Verze 3.1.1 - Podpora následujících modelů:

- 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)

2.1.4 Verze 3.0.1 - Podpora následujících modelů:

- 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 gen, 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 Důležité poznámky k vydání

3.1.1 Verze 3.5.0

Pozor – výrazná změna chování klasifikátorů.
Upgrade provede zjednodušení parametrů klasifikace. Blíže v detailním popisu nových funkcí v sekci 4.1.1

Pozor – možný upgrade firmware Dell PERC
Upgrade automaticky detekuje a v případě potřeby aktualizuje firmware Dell PowerEdge Raid Controlleru.

Vylepšení VMWARE a SQL komponent.
Nový blockly blok.
WES (LOGmanager Windows Event Sender) nově používá kryptografický protokol TLS 1.2.
Nové dashboardy a vzory upozornění.
Drobné opravy a vylepšení.

3.1.2 Verze 3.4.0

Korelace a Alerty s limity – Zvýšen maximální limit pro životnost kontextů z 15 na 30 minut.
Přidána možnost omezit překlad DNS PTR pouze na IP adresy, které jsou definovány v IP prefix listu.
Nové bloky.
Drobné opravy a vylepšení.

3.1.3 Verze 3.3.0

Pozor – změna chování čtení dat z Oracle databáze.
Po aktualizaci systému a komponent (komponenty by se měly aktualizovat do 30 minut po restartu do nové verze) si prosím zkontrolujte připojení k Oracle databázi. Bylo opraveno chování čtení dat z Oracle dle standardu. Pokud čtete data z Oracle pomocí synonym pohledů, je nutné dle dokumentace Oracle zadávat název tabulky resp. synonyma velkým písmem!

Přidána základní telemetrie produktu.
Počínaje touto verzí software je standardně zapnutá funkce odesílání statistik využití zařízení/funkcí zpět výrobci. Odesílaná data jsou v maximální možné míře anonymizovaná. Neobsahují žádné citlivé údaje ani konkrétní data, pouze informace o tom, jaké LOGmanager funkce jsou využívány a případně v jakém množství. Tuto funkci je možné vypnout v menu Uživatelé > Autentikace. Je zde viditelný i náhled dat, která jsou odesílána výrobci. Po aktualizaci na tuto verzi LOGmanager prvních 7 dní neodešle žádné informace. **Pokud je to možné, nechávejte sdílení statistik s výrobcem zapnuté. Umožní to vývojovému teamu LOGmanager lépe sledovat, na které funkce se soustředit s vývojem.**

Přidána podpora Office365.
Přidána podpora Syslog přes TLS.
Přidána podpora ověřování a šifrování SMTP.
Přidána podpora NXLOG agenta pro sběr logů z Windows prostředí.
Vylepšena podpora integrace se systémy SIEM/UBA třetích stran.
Drobné opravy a vylepšení.

3.1.4 Verze 3.2.4

Vylepšena funkcionalita clusteru.
Opraveno několik chyb způsobených možným předběhnutým startem jednotlivých služeb v systému (tzv. Race Condition).

3.1.5 Verze 3.2.2

Přepracována funkce operace clusteru.
Přidána podpora pro novou generaci demo boxů.
Pokud je v systému přítomen LOGmanager Workload Akcelerátor, je aktivován a příchozí data jsou automaticky primárně ukládána na NVMe SSD disk.
Přidána podpora pro zpětný import exportovaných událostí.
Optimalizace zabudovaných parserů.

3.1.6 Verze 3.1.1

Přidána podpora pro nové generace HP / Dell serverů. Nově všechny aktuální LOGmanager-XL modely obsahují nativně integrovaný Workload Akcelerátor (p/n: LOGmanager-A).

Přidána podpora pro snadné parsování strukturovaných dat dle rfc5424.
Přidána podpora pro zálohování dat.
Mnoho drobných vylepšení a oprav.

3.1.7 Verze 3.0.1

Přidána podpora funkce pro event correlator (thresholdy a korelace, tj. základní funkce SIEM).
V integrovaných templatech alertů jsou tři nové příklady:

- EC Deleted files on file server = detekuje, když nějaký uživatel smaže na fileserveru více jak 20 souborů.
- EC 50 bad logins followed by succesfull login = detekuje, když některý uživatel má více jak 50 neúspěšných přihlášení a pak se přihlásí úspěšně. Neboli detekce úspěšného slovníkového útoku.
- EC too many failed logins = detekuje, když se některý uživatel přihlásí více jak 5x špatně.

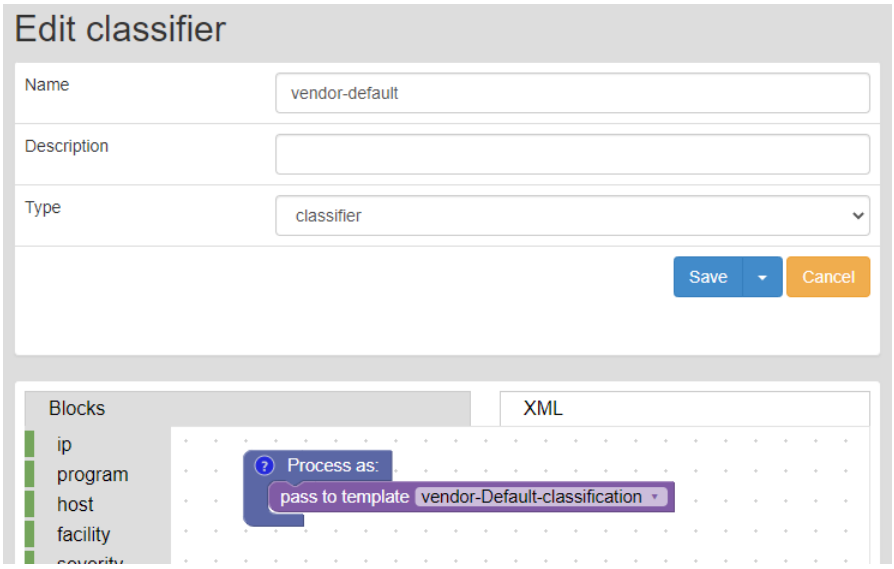
Všechny příklady si samozřejmě můžete upravit na základě vašich potřeb.
Upozornění: Zprávy, které používají contexty, jsou zhruba 4x náročnější na procesorový čas zpracování! Není například dobrý nápad počítat u logů z firewallu, kolikrát která IP adresa komunikovala…

Přepracované a aktualizované bloky.
LOGmanager verze 3.0.1 obsahuje velké množství změn a není možné provést downgrade na předchozí verzi bez obnovení zálohy! Doporučujeme provést před upgrade zálohu konfigurace.

4 Nové funkce

4.1.1 Verze 3.5.0

- **Pozor:** výrazná změna chování klasifikátorů. U klasifikace byl globálně odstraněn filtr na zdroj dat. Výsledkem úpravy je sjednocení pravidel tak, aby bylo možné pomocí jedné klasifikace třídit data ze všech zdrojů současně.
    - Při aktualizaci systému provede LOGmanager automaticky migraci vašeho nastavení klasifikace. Do všech vašich současných klasifikátorů bude automaticky vložena podmínka na zdroj vstupních dat.
    - Tato změna umožní výrazné zjednodušení klasifikace a značkování dat.
    - Přejmenování předdefinovaných klasifikátorů na vendor-*; pro jasnější rozlišení výrobcem vytvořených klasifikátorů od nově/uživatelsky vytvořených.
    - Doplnění a zjednodušení předdefinovaných klasifikátorů o další zdroje pro optimální funkčnost.
    - Všechny nově nainstalované LM od verze 3.5.0 obsahují pouze jeden defaultní klasifikátor, nazvaný vendor-default, který pošle všechna data do klasifikační šablony vendor-Default-Classification, která vyřeší parsování dat ze všech zdrojů.
        - Pokud používáte **nezměněnou** podobu klasifikátorů a chcete si zjednodušit klasifikaci, doporučujeme následující postup (POZOR: pokud máte provedeny změny v klasifikaci, berte tento postup pouze jako inspiraci pro možné zjednodušení!):
            1. Přejmenujte classifer syslog na vendor-default.
            2. Z XML smažte podmínku na zdroj syslog a upravte jej dle obrázku:



3. Smažte nepotřebné klasifikátory O365,checkpoint,vmware,sql. Všechno nastavení těchto klasifikátorů je nově přesunuto do vendor-Default-classification.

- **Pozor:** Chyba řadiče Dell PERC H470P do verze 50.5.1-2633:
    - Firmware řadiče obsahuje chybu, která může způsobit ztrátu dat při výměně poškozeného disku.
    - LOGmanager provede automaticky kompletní kontrolu RAID, upgrade firmware řadiče a následnou druhou kontrolu integrity dat. LOGmanager automaticky upozorní správce na nutnost restartovat server pro aplikaci nové verze firmware do řadiče = **zkontrolujte si prosím nastavení SMTP!**
    - Kontroly i automatický upgrade jsou spuštěny s nízkou prioritou, očekávejte výraznou prodlevu, než LOGmanager pošle žádost o restart.
- VMware komponenta:
    - Aktualizace pro správnou funkčnost i s VMware 7.x.
    - Vylepšené logování komponenty.
- SQL komponenta:
    - Přidána podpora pro čtení přesného času pro Oracle databáze.
    - Vylepšeno logování chyb a timeout operací.
- Vylepšení NTP. Nově obrazovka Přehled / Stav systému ukazuje okamžitý stav NTP procesu a synchronizace času.
- Upozornění na problém s automatickým zálohováním databáze. V případě, že je detekován problém s automatickým zálohováním databáze, je nově administrátor LOGmanageru informován emailem.
- Nový blockly textový blok „decamelize“. Příklad: text „SomeValueA“ převede na „some_value_a“.
- Windows agent začne po prvním připojení k LM serveru automaticky používat TLS 1.2 místo původní TLS 1.0, kterou MS dotnet automaticky preferuje.

- Nové/upravené dashboardy:
    - 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

Pokud je nutné pro získání dat provést dodatečnou konfiguraci na zdrojovém systému, dashboardy nově obsahují minimalizované pole s popisem potřebné dodatečné konfigurace zdrojového systému.

- Nové šablony upozornění:
    - 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

4.1.2 Verze 3.4.0

- Všechny nově přijaté zprávy mají vygenerované unikátní ID v poli meta.event@id
- Do vzorových alertů, které používají kontexty, byla přidána ukázka, jak využít event@id ke sledování událostí, které vstoupily do korelace.
- Zpřístupněny bloky pro parsování a psaní regulérních výrazů i v alertech a klasifikátorech.
- Přidán nový blok „in text replace“, který slouží k nahrazování textu.
- Přidána nová volba v blocích „raw_real“. Obsahem této proměnné je celá zpráva bez krácení automatickým offsetem. Vhodné pro zpracování zpráv, jejichž hlavička nedodržuje standardy.
- Přidána možnost omezit překlad DNS PTR pouze na IP adresy, které jsou definovány v IP prefix listu.
- Vylepšeno zobrazení klasifikátorů, zobrazení přehledu nově ukazuje detailnější zjednodušený pohled na to, co klasifikátor dělá.
- Zvýšen maximální limit pro životnost kontextů z 15 na 30 minut.
- Optimalizace parsovacích procesů při prohledávání IP prefix listů.
- Optimalizace cache regexů parsovacích procesů.
- Přidán nový dashboard pro Office365.

4.1.3 Verze 3.3.0

- Odesílání statistik o využití funkcí LOGmanageru výrobci. Co je odesíláno, je možné zobrazit a funkci případně vypnout v menu Uživatelé > Autentikace. Zařízení neodešle žádná data první týden od startu systému. Prosíme, pokud je to možné, nechávejte tuto funkci zapnutou.
- Přidána podpora pro Office365. Získávání logů z Microsoft cloud prostředí.
- Přidána podpora pro SMTP ověřování a šifrování spojení se SMTP serverem.
- Přidána podpora pro příjem logů z NXLOG agenta, LOGmanager se k těmto logům chová stejně, jako kdyby byly přijaty z nativního Windows agenta (přidávání tagů, automatický expand JSON v classifiers apod.)
- Přidány chybějící bloky do Alertů – všechny sekce zpracování dat nyní obsahují stejné bloky.
- Přidána podpora pro příjem logů pomocí TLS syslog.
- Přidána upozornění při sestavováni clusteru s informací, že všechna data na "slave" systému budou smazána.
- Přidáno uživatelské pole description k tagům.
- Syslog output nově umožňuje nastavit 4 různé formáty přeposílaných zpráv. Tato možnost přináší snazší integraci s nadřazenými SIEM/UBA systémy třetích stran. (IBM QRadar apod.)

4.1.4 Verze 3.2.4

- Žádné nové funkce.

4.1.5 Verze 3.2.2

- Přepracována funkce operace clusteru. Podrobné informace jsou v dokumentaci popisu clusteru: naleznete zde.
- Přidána podpora pro zpětný import exportovaných událostí.

    - LM si z externího SMB serveru stáhne vytvořenou zálohu a naimportuje jí zpět do systému.
    - Všechna zpětně importovaná data jsou označena.
    - Importovaná data nejsou ze systému automaticky odmazána, musí být ručně smazána z Database status stránky.
    - Aktuálně je podporován pouze jeden současný import, pro import více dnů je nutné počkat na doběhnutí úkolu a teprve poté zadat další import.
- Přidána podpora pro zabudovaný LOGmanager Workload Akcelerátor v nové generaci LM boxů. Nově jsou spuštěny dvě instance databáze, jedna instance na HDD a jedna instance na NVMe. Všechna příchozí data jsou indexována na NVMe, po provedení optimalizací jsou data automaticky přesunuta na HDD.
- Parsovací engine nově používá optimalizaci běhu u všech zabudovaných parserů. Interní, tj. LOGmanager vývojovým teamem vytvořené, parsery díky této optimalizaci spotřebují o 20-50 % méně CPU na vlastní parsovací operace.
- Cluster nově provádí periodické kontroly integrity clusteru (postupně otevírá, kontroluje a následně zavírá historicky uložená data). Původně se toto dělalo pouze při startu systému, nově je tato funkce rozložena v čase.
- Přidán nový interní monitoring, v dalších verzích budou postupně zpřístupněny grafy zátěže, počtu zpráv apod. v dashboardech provozního stavu LM.
- Přidán API endpoint pro vytvoření support balíku na vyžádání. Balík obsahuje výstupy diagnostických příkazů, interní logy aplikací a částečnou konfiguraci (balík neobsahuje žádné citlivé údaje = hesla uživatelů/AD/komponent ani SSL certifikáty).
- Optimalizace běhu interních front, dvojnásobné zrychlení příjmu vstupních dat do parserů.
- Optimalizace automatického otevírání a zavírání historických dat. Prohledávání dat starších 8 dní bylo zrychleno o 5-30 vteřin.
- SQL komponenta – přidána podpora pro sběr událostí v tabulkách, které používají datetime2.
- Přidán dashboard pro Squid.

4.1.6 Verze 3.1.1

- Přepracována stránka zobrazení Database status. Nově zobrazuje stav všech denních indexů, které jsou v LM uloženy, a umožňuje ručně otevírat a zavírat indexy pro jednotlivé dny.
    - Dashboardy se i nadále automaticky starají o otevírání indexů, nově po prohledání dat index i automaticky zavřou. Pro vyhledávání dat není vyžadováno indexy ručně otevírat.
    - Každá akce vyhledávání v databázi nově vytváří zámky databáze. Zámky se vytváří pro systémové i uživatelské dotazy. Pokud na indexu existuje zámek, není možné jej zavřít. Neobnovené zámky se automaticky uzavřou po 4 hodinách.
    - Systém nově nedovolí otevřít a prohledat více dat, než je velikost dostupné operační paměti.
    - Přidáno tlačítko pro export zálohy vybraných denních indexů na externí SMB server.
- Přidána podpora pro sběr a parsování logů ve strukturovaném formátu dle rfc5424.
- Testovací okno pro psaní parserů nově podporuje vkládání celé syslog zprávy, bez nutnosti ořezávat zprávu o vypočítaný raw_offset. Offset se nyní vypočítá automaticky a je možné pracovat i se standardní syslog hlavičkou (programname apod.).
- Přidána podpora pro archivaci dat na externí SMB úložiště. Dle nastavení se pro každý den (dle UTC času) provede export událostí z předchozího dne na definovaný SMB server. Zálohy jsou kompresovány GZip algoritmem.
- Změna hostname LOGmanageru. Původní hodnota byla "LOGmanager", novou hodnotou je sériové číslo LOGmanageru, tak aby šlo snadno rozlišit, o jaký systém v clusteru se jedná.

4.1.7 Verze 3.0.1

- Přidán korelátor událostí (upozornění s limitní hodnotou [alert with threshold] a korelace).
    - Přidána definice kontextů a času jejich životnosti v rozsahu 60 až 900 sekund.
    - Přidány nové vzory pro Alerty s kontexty.
- Parsery a alerty nově umožnují použití matematických operací.
- Parsery a alerty nově podporují dekódování URL (scheme, netloc, path, params, query, fragment, hostname, username).
- Přidán blok, který umožnuje přijatou zprávu zahodit.
- Přidána podpora pro multicolumn lookup tabulky.
- Odstraněna funkce doplnění názvu města k IP adresám, vysoká nepřesnost u jednotlivých IP adres (zdůvodnění: více jak 90% měst bylo určováno s velmi nízkou přesností).
- Přidána podpora pro novou generaci serverů Dell (-G2).
- Zvýšen počet parsovacích procesů o 40%.
- Přidáno tlačítko na deaktivaci automatického překladu DNS PTR záznamů u IP adres. V případě logování velké části provozu z firewallu docházelo díky zpoždění DNS a čekání na odpovědi k výraznému zpomalení parsovacích procesů. V extrémních případech logování IP adres, u kterých neexistovaly/neodpovídaly DNS servery, dochází až k 90% zpomalení parsovacích procesů.
- Checkpoint – aktualizace OPSEC SDK.
- Checkpoint – přidán interní ping v rámci OPSEC protokolu pro kontrolu stavu komunikace v rámci OPSEC tunelu.

5 Nové parsery:

5.1.1 Verze 3.5.0

- Nové parsery:
  - Oracle audit db
  - Windows DNS debug log
  - AIP-safe
  - Bash
- Aktualizované parsery:
  - Fortimail – standardizace názvů polí, rozšíření podpory pro nové verze Fortimail OS
  - O365 – vylepšené parsování
  - Windows – nově jsou parsována data o instalaci KB a Terminal server operacích
  - Tomcat – přidána podpora pro sběr z windows

5.1.2 Verze 3.4.0

- Aktualizované parsery:
  - Windows – oprava špatného tagování loginfailed
  - PaloAlto – podpora pro BSD formát
  - ArubaOS – podpora pro příjem zpráv v CEF formátu od verze Aruba 8.x
  - Optimalizované parsery pro využití nově přidaných bloků: Huawei, Sophos, Juniper, Exchange, epacs, Checkpoint, Greycortex, PaloAlto, Aruba

5.1.3 Verze 3.3.0

- Nové parsery:
  - Greycortex
  - Radware Defens Pro
  - F5 ASM
  - Cisco ISE
  - Cisco UCS
  - Office365
  - ePacs
- Aktualizované parsery:
  - Safetica DLP
  - Synology DSM – podpora pro příjem strukturovaných logů
  - Windows – aktualizovány tabulky pro překlad chyb s přihlášením, oprava tagů.
  - Squid
  - Mikrotik
  - Cisco-asa podpora pro Firepower
  - HP-Aruba
  - HP iLO
  - Flowmon
  - Palo Alto
  - Checkpoint
  - SSH

5.1.4 Verze 3.2.4

- Nové parsery:
  - Safetica DLP
  - Synology DSM
- Aktualizované parsery:
  - Microsoft Windows – opravena chyba špatně tagovaných "login failed" zpráv s EventID:4776 pro status: 0x0.
  - Mikrotik – podpora pro parsování DHCP a forward zpráv

5.1.5 Verze 3.2.2

- Nové parsery:
  - Symantec Endpoint Protection Manager
  - Symantec Messaging Gateway
  - Squid
  - Junipersrx structured data log
  - Junipersrx-lite
  - Barracuda Email Security Gateway
- Aktualizované parsery:
  - Microsoft Sharepoint
  - Windows-firewall - kompletně přepsaný, optimalizovaný na výkon
  - HPE - Comware OS
  - Squid - přidána podpora pro sběr logů z Windows prostředí
  - Huawei USG
  - Windows
  - Unifi
  - Cisco IOS
  - Cisco ASA
  - Palo Alto

- Proběhla normalizace všech emailových adres napříč všemi parsery.

5.1.6 Verze 3.1.1

- Nové parsery:
  - FortiManager
- Aktualizovány všechny integrované parsery. Zlepšení a optimalizace práce s parsováním zpráv. V příští verzi LM bude aktivována funkce, která u všech integrovaných parserů zrychlí parsování zpráv o 20-50%.

5.1.7 Verze 3.0.1

- Nové parsery:
  - FortiGate-lite
    - odlehčená verze parseru, který parsuje jen vybraná pole.
    - Parser je o zhruba 30% rychlejší než normální fortigate parser.

        - Vybraná pole: 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
- Aktualizované parsery:
    - HP Comware
    - FortiGate
        - Parser nově neparsuje další duplicitní nebo neužitečná pole (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 nově zpracuje i logy přijaté přes syslog (BSD formát)
    - Trapeze
    - LOGmanager
    - Kaspersky - parser nově zpracuje i logy přijaté ve formátu CEF
    - FortiMail
    - JuniperSRX
    - Cisco SMB
    - Cisco IOS

6 Opravené chyby

6.1.1 Verze 3.5.0

- Upozornění (Alert) neodeslalo email v případě špatně nadefinované formátovací template. Nově je poslána emailem informace o špatné konfiguraci a událost, která toto způsobila.
- Nově použitý NTP Daemon Chrony umožňuje stabilnější synchronizaci s nativní (nikoliv exaktní) NTP implementací Microsoft serverových operačních systémů. (Nejedná se o chybu v pravém slova smyslu, ale vylepšení, ke kterému jsme nuceni nestandardní implementací NTP Microsoft).

6.1.2 Verze 3.4.0

- Syslogforwarder mohl při určité kombinaci českých znaků nepřeposlat syslog zprávu.
- Opravena chyba, kdy při ručním dotazování web-api byla vracena chyba „Error.“ Nově je informace doplněna o detailnější informace.
- Oprava řazení windows agentů = nově je funkční řazení agentů dle času, kdy se naposledy připojily.

- Odebrána možnost procházet IP prefix list pomocí bloku "foreach". IP prefix listy je možné používat pouze s blokem "if in", jak je popsáno v dokumentaci.
- Opraven dashboard pro Juniper a některé template alertů.

6.1.3 Verze 3.3.0

- Opravena chyba „race condition“, kdy při startu systému mohlo za určitých okolností dojít ke startu systémových služeb dříve, než byly dostupné disky.
- Opravena chyba nezobrazení IP adres na konzoli LOGmanageru, ke které docházelo v případě určitého nastavení IP adres.
- Opraveno špatné escapovaní Unicode regulárních výrazů v Parserech. Nově je možné používat jakékoliv Unicode znaky uvnitř Regex.
- Opraven SQL konektor – za určitých podmínek nerespektoval změny konfigurace v GUI a běžel stále se starou konfigurací.
- SQL konektor nemusel korektně číst logy z MSSQL serveru, kvůli špatnému ukončování transakcí.
- Opraveny odkazy na dokumentaci v dashboardech.
- SQL konektor se za určité konfigurace odmítal připojit k Oracle serveru. Upraveno vnitřní chování konektoru. **Pokud jsou čtena data ze synonym místo SQL tabulky je nově nutné specifikovat název synonym v UPPER CASE formátu dle standardu Oracle.**
- Opraveny odkazy na dokumentaci v dashboardech.
- Vylepšen Regex substituce pro detekci a normalizaci MAC adres.
- Opravena chyba konfigurace SMTP způsobující možně odeslání notifikací přes jiný než v konfiguraci definovaný SMTP server. Nově se použije vždy definovaný SMTP server.
- Opravena chyba VMWare konektoru, kdy za určitých okolností mohl přestat číst logy.
- Opraveno generování reportů. Pokud bylo velké množství reportů generováno v jednom krátkém časovém úseku, mohlo dojít k odeslání některých reportů bez naplnění daty.

6.1.4 Verze 3.2.4

- Verze 3.2.2 neměla v případě ztráty master serveru a rozpojení clusteru dostupná uložená data.
- Při spojování boxů do clusteru jsou nově všechna data na "slave" boxu při připojení automaticky smazána.
- Race condition, kdy předčasná aktivace Workload Akcelerátoru mohla způsobit nakopírování starých indexů na Workload Akcelerátor, kde tím došlo k zaplnění úložného prostoru. Nově příchozí data byla stále korektně zpracována, ale byla ukládána na HDD místo zpracování na Workload Akcelerátoru. Nedošlo ke ztrátě dat.
- Race condition, aplikace pro ukládání událostí do databáze mohla při specifické kombinaci několika okolností skončit chybou databáze. Nově příchozí data byla ukládána do vyrovnávací paměti až do jejího zahlcení a po zahlcení mohlo dojít ke ztrátě dat.

6.1.5 Verze 3.2.2

- Opravena chyba nastavení SMB protokolu v LM, používal se defaultně starý SMB protokol.
- Opravena chyba, kdy po spojení LM do clusteru bylo nutné ručně restartovat slave box. Nově se slave box automaticky restartuje při připojení do clusteru.
- Opravena chyba znemožňující modifikaci SSL/RELP certifikátu.
- Opravena chyba, kdy bylo možné chybou uživatele vytvořit smyčku v certificate chain.

- Opraveno zobrazení popisu databázové skupiny.
- Opraveno zobrazování dat v dashboardech (v případě, že prohledávání topN událostí bylo prováděno nad více dny, mohlo dojít v případě chybějících vyhledávaných dat v nějakém dnu k zobrazení chybové hlášky místo očekávaného výsledku).
- Postfix opraven špatně nastavený hostname.
- Opravena chyba, kdy při nedostupném SMB serveru nebylo možné tuto konfiguraci změnit.
- Opraveno zobrazení stránky Database status pro prohlížeč Edge.
- Opravena uživatelská oprávnění pro editaci LDAP skupin.

6.1.6 Verze 3.1.1

- Opravena chyba vyhledávání v dashboardech, která mohla v ojedinělých případech vést k pádu systémové databáze. Projevit se mohla na velmi vytížených systémech při prohledávání dat v dlouhém časovém úseku.
- Opraveny bezpečnostní zranitelnosti vyplývající z ohlášených zranitelností Linux kernelu CVE-2018–5390.
- Odstraněna HTTP HSTS hlavička vynucující Strict-transport-security. Hlavička říká prohlížeči, že se nesmí připojit na webserver, pokud má expirovaný HTTPS certifikát. V případě expirace uživatelsky nahraného certifátu, není při použití této hlavičky možné změnit a obnovit certifikát, protože prohlížeč odmítne zobrazit jakékoliv stránky systému.
- Opraven příkaz traceroute v CLI.
- Opraveno zobrazování a escapování dashboardů. Tato chyba umožňovala v prostředí dashboardů spustit JS kód, podvržený do systémem přijaté syslog zprávy. Nově jsou všechny HTML znaky v přijatých zprávách escapovány.
- Opravena chyba parsovacího procesu, který skončil chybou při nekorektním zadání regulárního výrazu. Nově je zobrazena chybová hláška o špatně vytvořeném regexu.
- Opravena chyba testovacího okna alertů. Vložená testovací zpráva, která obsahovala tag o tom, že byla alertována, zobrazovala chybně vždy informaci o tom, že bude alertována. Nově je zobrazena informace, pouze pokud se splní všechny zadané podmínky alertu.
- VMware komponenta nyní korektně přidává tagy.

6.1.7 Verze 3.0.1

- Aktualizace linuxového jádra na verzi s integrovanou ochranou proti útokům Meltdown/Spectre. Na LOGmanager není a nebylo možné zaútočit ani jedním z těchto útoků. Podrobné vyjádření k těmto zranitelnostem je k dispozici na uživatelském fóru LOGmanager.
- V určitých případech bylo nefunkční přidávání tagů k windows agentům.
- Vylepšeno interní logování syslog forwarderu (connection timeout, connection reset apod.).
- Opravy parsovacího procesu, přidána řada dalších upozornění na možné chybové stavy při zpracování zpráv.
- Exportování událostí na velmi vytíženém boxu nefungovalo vždy spolehlivě.
- Úprava oprávnění pro stahování Windows agenta, nyní jej může stáhnout kdokoliv, kdo má oprávnění na sekci Windows.
- SQL – Opraveno občas nefunkční připojení na Microsoft SQL server instance.
- SQL – Opraveno možné excesivní logování nepřipojeného SQL agenta.

7 Známé chyby

7.1.1 Verze 3.2.4, 3.3.0, 3.4.0.

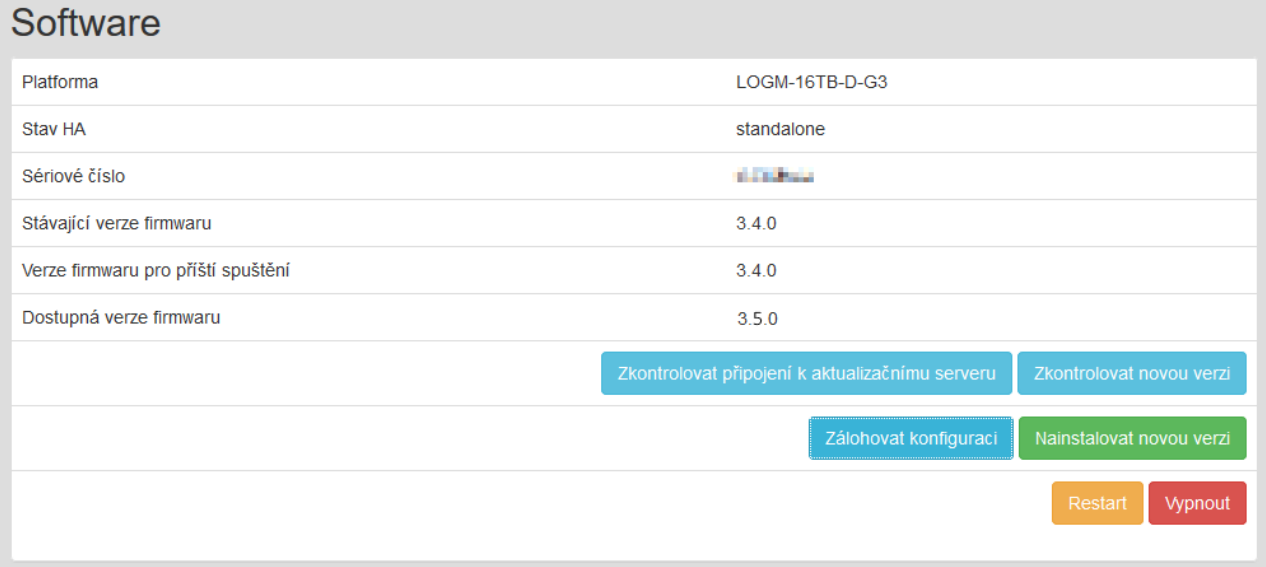
- Problém:
  - Editace databázového oprávnění občas nenačte bloky. Projevuje se primárně v Chrome.
- Workaround:
  - Znovu načíst stránku.

- Problém:
  - Editace databázového oprávnění občas nezobrazí přeložené názvy tagů.
- Workaround:
  - Přepnout na xml zobrazení a zpět, tagy se přeloží.

8 Postup aktualizace

UPOZORNĚNÍ: Release 3.5.0 NEPODPORUJE postupný upgrade clusteru. Aktualizaci clusteru je nutné provést instalací nového SW na oba boxy a současný restart obou nodů v clusteru.

Pro instalaci nové verze klikněte ve webovém rozhraní na Systém > Software
Otevře se stránka s informací o nainstalovaném software



Postup upgrade:

- Klikněte na tlačítko „Zkontrolovat novou verzi“.
- Zobrazí se dostupná verze **3.5.0.**
- Klikněte na tlačítko „Zálohovat konfiguraci“ pro uložení konfigurace před upgrade.
- Klikněte na tlačítko "Nainstalovat novou verzi".
- Po opětovném načtení stránky se v next boot firmware zobrazí **3.5.0.**
- V posledním kroku stačí kliknout na Restart a systém se restartuje do nové verze.

8.1.1 Po restartu serveru

Po restartu serveru je nutné, pro korektní funkci webového rozhraní, vymazat cache prohlížeče!

Po každé aktualizaci je provedena kontrola integrity databáze, po restartu serveru je stav databáze vždy ve stavu red, a je prováděna kontrola – je to tedy normální stav po upgrade, po dokončení kontroly se stav vrátí do normálního stavu.
Po dobu provádění kontroly integrity nejsou do DB ukládána nová data! Přijaté události nicméně zůstávají v interní cache a jsou do DB vloženy ihned po dokončení kontroly. Kontrola může v závislosti na velikosti a množství uložených událostí trvat až 30 minut.

Konec dokumentu.