LOGmanager - release notes – verze 3.8.0

Verze:	3.8.0	**Datum:**	31.01.2022

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 3.7.0 a 3.8.0

- 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)
- LOGM-192TB-D-G3 (2U Dell R740xd, 12x 16TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-96TB-D-G3 (2U Dell R740xd, 12x 8TB HDD, 128GB RAM, 2x12core CPU)

3 Důležité poznámky k vydání

3.1.1 Verze 3.8.0

Hlavní novinkou této verze je nový systém pro sběr logů z Windows prostředí prostřednictvím nového agenta postaveného na OpenSource Beat. Zvýšení výkonu, interoperability a stability při zachování všech dosavadních možností předchozího agenta LOGmanager WES.

Přidána podpora pro sledování zdrojů. Administrátor bude na základě pravidel upozorněn na situaci, kdy vybraný zdroj přestane odesílat logy.

Vyměněn a vylepšen interní systém pro správu úloh.

3.1.2 Verze 3.7.0

Přidána podpora pro příjem a parsování dat z winlogbeat a filebeat.
Přepracované a upravené defaultní dashboardy.
Výměna interního monitoring systému.
Přidána podpora pro postupný upgrade clusteru.
Kompletně přepracován návod „Microsoft Security Auditing for LOGmanager“.

3.1.3 Verze 3.6.2

Přepracované kontexty, opravena chyba v matematických operacích uvnitř kontextů.

3.1.4 Verze 3.6.1

POZOR – Toto vydání obsahuje upozornění na plánované ukončení podpory CheckPoint komponenty na stahování logů prostřednictvím OPSEC protokolu. Informaci, jak CheckPoint Firewally nastavit pro použití **CheckPoint log export** komponenty, naleznete v naší dokumentaci. Prosíme zákazníky, kteří využívají CheckPoint sběr logů prostřednictvím nastavení v menu Zdroje/CheckPoint, aby si do příští verze LOGmanager software změnili konfiguraci.

Odlehčené parsery. Nově je dostupné snadné zapnutí odlehčených („Lite“) parserů bez nutnosti upravovat klasifikaci dat. Pro velmi vytížené boxy je vhodné začít tyto odlehčené parsery používat. Během zpracování dat totiž generují menší množství polí, což sníží náročnost na CPU, kapacitu diskového pole i paměti systému.

Testovací okno (známé z parserů a upozornění) nově i v klasifikaci vstupních dat.
Pole typu IP adresa nově obsahuje sub-pole s číslem a názvem AS (autonomního systému).
Digitální podepisování záloh. Vylepšení efektivity zálohovacího subsystému na velmi vytížených boxech.
Vylepšení RBAC (Role-Base Access Control) funkce pro navýšení množství souběžných operátorů systému.
Optimalizace práce interních vyrovnávacích front.
Optimalizace a zrychlení zpracovávání dat v clusteru – navýšení výkonu o 30-40 % a replikace dat o 75 %.
6 nových a 9 upravených parserů, 6 nových dashboardů.
Přidána kompletní podpora pro nové generace serverů (G3).
Další drobné opravy a vylepšení.

3.1.5 Verze 3.5.2

POZOR – Tento release obsahuje opravy chyb verze 3.5.0. Pokud používáte verzi 3.5.0, doporučujeme provést aktualizaci v nejbližší možné době!

Toto vydání obsahuje opravu chyby, která by mohla za určitých, málo pravděpodobných okolností způsobit pád služeb celého systému.

3.1.6 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.

3.1.7 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.

3.1.8 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.

4 Nové funkce

4.1.1 Verze 3.8.0

- Nová verze agenta pro sběr logů z prostředí Microsoft Windows – Beat s kompletní podporou minimálně na úrovni předchozího WES agenta.
    - Původní verze sběru logů ponechána, pouze jméno doplněno o „legacy“.
    - Nové MSI pro sběr logů z Windows prostředí – LOGmanager Orchestrator. K dispozici ve dvou verzích, s podporou automatické aktualizace a bez podpory automatické aktualizace.
    - Komunikace Beat agenta s API LOGmanageru TLS 1.2, odesílání logů z Beat agenta TLS 1.3.
    - Komunikace Beat agenta vyžaduje striktní používání DNS jména v SRV Type záznamu pro službu automatické konfigurace agenta.
    - Přidána kompletní konfigurace v následujících menu: Zdroje > Beat agenti / Beat filtry / Beat globální konfigurace.
    - Přidána funkce pro filtrování logů odesílaných novým Beat agentem.
    - Podpora manuálního nastavení DNS jméno LOGmanageru pro odesílání logů mimo doménu v registry.
    - Nová dokumentace včetně popisu nastavení registry na hostech s Beat agentem.
    - Vytvořeno nebo aktualizováno 8 parserů pro zpracování logů z prostředí Microsoft pro logy odesílané Beat agentem. Zpřehledněna a vylepšena vendor klasifikační šablona pro logy z Beat agentů.

  Poznámka: Automatická aktualizace WES -> Beat: *Nová verze agenta z důvodu velkého množství změn prozatím neumožňuje automatickou aktualizaci a migraci konfigurace. V tuto chvíli doporučujeme postupně migrovat na novou verzi agenta alespoň u vybraných systémů s velkou zátěží nebo systémů, které stojí mimo doménu a požadují manuální konfiguraci adresy LOGmanageru.*
  Důležitá poznámka: *Automatická konfigurace agenta a DNS záznam: Před zahájením používání Beat Agenta prosím zkontrolujte, zda máte v DNS SRV Type záznamu použito DNS jméno LOGmanageru, nikoliv jeho IP adresu. Pokud zůstane v DNS SRV Type záznamu pro LOGmanager uvedena IP adresa, Beat agent odmítne odesílat logy. Důvod – používání certifikátů pro ověřování identity neumožňuje používání IP adres.*

- Přidána funkce pro sledování zdrojů a příslušné GUI rozhraní
    - Tato funkce umožňuje na základě jmen (hostname) sledovat a upozorňovat na zdroje logů, které přestaly odesílat data do LOGmanageru. Nové GUI rozhraní naleznete v menu Logy > Sledování zdrojů.

- Vyměněn interní systém, který spouští interní úlohy.
    - Nově jsou v GUI zobrazeny informace o stavu interních úloh v menu Systém > Stav systémových úkolů.
    - Jsou zobrazeny exporty databáze a jejich aktuální stav.
    - Přidány automatické alerty pro případ, že export databáze nebylo možné dokončit.
    - Změněno flow pro exporty databáze, před exportem se nejdříve zjistí, zda je možné připojit se na SMB server a zda server obsahuje dostatek místa.

- Přidána možnost automaticky odesílat chyby vzniklé při běhu LM směrem k výrobci. Defaultně vypnuto.
- Dockerizace interních komponent.
- Nová verze rsyslog.
- Vrácena zpět informace o IP adresaci iLO/iDrac LOGmanageru v menu Přehled > Stav systému.
- Nové dashboardy:
    - ISO Access Provisioning
    - Microsoft Exchange
    - DNS overview
    - Zyxel DHCP log
    - Zyxel Interface statistics log
    - Zyxel Performance log
    - Zyxel SSL VPN log
    - Zyxel System log
    - Zyxel Traffic log
    - Zyxel Webfilter log
    - Zyxel WLAN log
- Opravené/vylepšené dashboardy:
    - Dell servers iDRAC
    - Windows DHCP
    - Windows DNS

4.1.2 Verze 3.7.0

- Přidána podpora pro příjem logů z winlogbeat a filebeat
    - Pouze šifrovaný příjem dat pomocí TLS1.3
    - JSON Data přijatá z beatů jsou automaticky expandována do proměnné msg[“structured_data”]. Data lze použít přímo v klasifikaci, testovací okna podporují data z beatů.
- Vyměněn interní monitoring systém
    - GUI zobrazuje grafy využití CPU
    - Vylepšeno zobrazování síťových interface a link agregací
- Přidána podpora pro několik dalších formátů syslog output pro zjednodušení integrace s řešením qradar.
- Přidána podpora pro postupný upgrade clusteru.
- Kompletně přepracován návod „Microsoft Security Auditing for LOGmanager“.
- Aktualizovány příklady korelací alertů o nové možnosti korelací přidané ve verzi 3.6.2
- Přidána podpora pro čtení logů z vmware verze 7.0.2
- Přepracována domovská stránka s dashboardy.
- Nové dashboardy:
    - ISO Access Provisioning
    - ISO Authentication
    - ISO File Access
    - ISO Network Monitoring
    - ISO User Accounts
    - ClearPass audit log

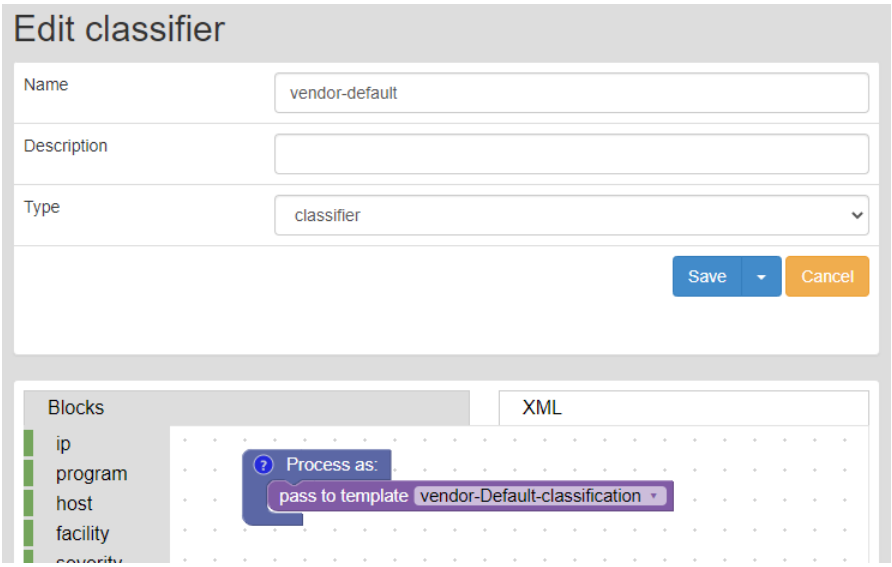
    - ClearPass endpoint log
    - ClearPass radius and accounting log
    - ClearPass radius log
    - ClearPass system log
    - ClearPass TACACS+ log
    - FortiGate DoS policy
    - FortiGate Antivirus
    - FortiGate DLP
    - FortiGate WAF
    - FortiGate users report
    - FortiADC attack log
    - FortiADC system log
    - FortiADC traffic log
    - FortiAuthenticator auth log
    - FortiAuthenticator config changes
    - FortiSandbox alert events
    - FortiSandbox debug events
    - FortiSandbox system events
    - FortiWeb attack log
    - FortiWeb system log
    - FortiWeb traffic log
    - MS Hyper-V overview
    - QNAP storage
    - SQL connector overview
    - HPE IMC
- Opravené/vylepšené dashboardy:
    - Squid proxy
    - Webservers access log
    - ISC DNS server
    - CEF overview
    - Fortigate IPsec

4.1.3 Verze 3.6.2

- Kompletně přepsána práce s kontexty
    - 2x rychlejší zpracování alertů používajících kontexty.
    - Nově je kontext při zpracování zprávy uzamčen. Pokud dojde k paralelnímu přístupu do stejného kontextu, druhý proces čeká na zpracování prvním procesem, než zprávu zpracuje (toto je možné zapnout díky výraznému zrychlení práce s kontexty). Není nově nutné předvídat hodnoty v kontextech, jelikož v kontextu budou vždy uložena přesná čísla počtu výskytů apod.
    - Přepracována interní práce s objekty @int, @float, nově je v textové reprezentaci objektu uložena string reprezetnace číselného objektu (dříve toto mohlo působit zmatečně při počítání v kontextech, kdy například hodnota count = 2 a hodnota count@int =3. Nově budou obě čísla stejná.

4.1.4 Verze 3.6.1

- Vyčítání logu z CheckPoint pomocí komponenty/LEA protokolu bylo označeno jako EOL a bude odstraněno v příští verzi. CheckPoint logy je nově možné zasílat pomocí Syslog nebo Syslog přes TLS, dle návodu v dokumentaci LM.
- Přidáno testovací okno zpráv do klasifikátorů. Poznámka: V této verzi kódu okno ověřuje způsob klasifikace pouze proti bloku v daném okně klasifikace/klasifikační šablony.
- Přidána další sada tzv. lite parserů, které parsují jen nejdůležitější informace. Nastavení, jak se budou data parsovat, je nyní možné provést v lookup tabulce Lite-parser-Settings. Použití lite parseru může hlavně u windows logů přinést zrychlení systému a výrazné snížení velikosti denních indexů. (Příklad pro Windows logy – efektivita použití „microsoft-windows-lite“ parsovacího pravidla: o 50% menší velikost denních indexů, o 75% menší paměťová náročnost a o 20% rychlejší indexace.)
- Zkrácena doba systémového skriptu, který se stará o replikaci dat v rámci clusteru. Původně otevíral a zavíral staré indexy každou hodinu, nově tuto operaci provádí každých 15minut. Tato změna výrazně zrychlí synchronizaci nových clusterů.
- Přidána funkcionalita ip2asn, ke všem IP adresám je nově automaticky doplněno číslo AS (autonomní systém) + název AS, pro větší efektivitu bezpečnostních analýz a statistik.
- Přidána funkce automatického podepisování exportovaných záloh databáze pomocí podpisů za využití 4096bit certifikátů vygenerovaných v LM při startu systému (detailně popsáno v dokumentaci).
- Zkráceno množství automaticky otevřených denních indexů z 8 na 6. Tato změna přináší výkonové zlepšení a možnost prohledávat větší množství historických dat na velmi vytížených LM.
- Vylepšení indexovacího výkonu clusteru o 30 až 40 % proti samostatně běžící jednotce. Jednotlivé nody v clusteru si nově automaticky rozkládají indexovací zátěž.
- Výrazná optimalizace interního systému front, nově optimalizované fronty potřebují pro svůj provoz zhruba 10x méně IO operací. Toto vylepšení přináší velké zlepšení výkonu zařízení ve chvíli, kdy frontuje.
- Nově budou všechna upravovaná nebo nově vytvářená parsovací pravidla obsahovat v popisu informaci o posledním datu aktualizace a testované verzi software zdrojového systému, pro který je dané pravidlo napsané.
- Přidáno nové RBAC oprávnění v systémových skupinách (vyhledávání/jen ke čtení), které dovolí uživateli s danou systémovou skupinou prohledat pouze data aktuálně otevřených indexů. Vhodné pro operátory, kteří nepotřebují nebo nemají vidět historická data systému.
- Přidána kompletní podpora pro novou generace serverů. LOGmanager SKU končí na G3.
- Nové/upravené dashboardy:
    - Dell iDrac
    - Synology NAS
    - Veeam
    - VMware status change
    - VMware user session
    - VMware overview
    - CEF Flowmon
    - FortiGate traffic log
    - Windows update



4.1.5 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

4.1.6 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.

4.1.7 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.)

5 Nové parsery:

5.1.1 Verze 3.8.0

- Nové parsery:
  - Beat-exchange
  - Siemens-scalance
  - Vectra-cognito
  - Zyxel
- Aktualizované parsery:
  - Beat všechny parsery – unifikace názvů polí s původními WES windows parsery.
    - Přidáno pole systemtime
    - Oprava logontype
    - Oprava restart reason
    - Přidána podpora pro sběr textových logů
    - Oprava windows uptime
  - Cisco-ios – Přidána podpora pro sběr logů z Wireless controlleru s IOS OS.
  - Fortiauthenticator – Přidáno extrahování detailnějších logů ze status.
  - Huawei – Vylepšení parsování ACL logů
- Změny klasifikace:
  - Nová klasifikační šablona vendor-beats-template provádí automatickou klasifikaci pro všechny továrně dodávané parsery. Před konfigurací nového Beat agenta pro sběr textových logů se podívejte do této klasifikační šablony, jak správně přiřazovat tagy pro textové soubory DHCP, DNS, Exchange a IIS logů.

5.1.2 Verze 3.7.0

- Nové parsery:
  - Beat-microsoft-iis
  - Beat-win-dhcp
  - Beat-win-dns
  - Beat-win-fileaccess
  - Beat-win-firewall
  - Beat-win-rdp
  - Beat-windows
  - Clearpass
  - Fortiadc
  - Fortisandbox
  - Fortiweb
  - Icewarp
  - Pulse secure
  - Qnap
  - Zimbra
- Aktualizované parsery:
  - Checkpoint - parser mohl za určité konfigurace vytvářet invalid pole.
  - Cisco-asa - aktualizováno o parsování ACL logů.

- Cisco-ios - přidáno parsování ACL logů.
- Cisco-ios-xe – přidána podpora pro nový Cisco formát.
- Firepower - přidán chybějící firewall tag.
- Flowmon - přídána podpora pro IDS logy.
- Freeradius - přejmenováno pole auth_method na authenticationtype, pro sjednocení s NPS a clearpass parserem.
- Huawei - podpora pro parsování logů z firewallu USG.
- Nginx - přejmenováno pole status na status_code, pro sjednocení s IIS parserem.
- Pulse secure - přejmenováno pole src_ip VPN logů na remote_ip (unifikace se zbytkem parserů).
- Samba - přidána podpora pro novější verze, unifikace názvů polí s windows parserem pro file audit.
- Sophos - přidány tagy loginfailed, loginsuccess, failed. Oprava názvu polí na standardní formát msg.rx > msg.rcvd_byte, msg.tx > msg.sent_byte. Podpora parsování MTA logů.
- Symantec-edr - přidána podpora pro novější formát logů.
- Vmware, microsoft - přidán tag virtualization.

5.1.3 Verze 3.6.2

- Aktualizované parsery:
  - Huawei
  - Windows DHCP
  - ArubaOS – přidána podpora pro SDWAN
  - Microsoft IIS
  - Postfix
  - Openssh
  - Cron
  - HP Comware
  - Brocade
  - Dell iDrac
  - Cisco IOS
  - Linux iptables
  - Windows RDP
  - Cisco ASA
  - FortiGate-lite
  - Windows-lite

5.1.4 Verze 3.6.1

- Nové parsery:
  - Windows lite
  - Cisco ASA lite
  - Veeam Backup & Replication
  - Hillstone NGFW
  - Microsoft Exchange tracking log
  - Pulse Secure
- Aktualizované parsery:
  - Huawei – doplněny nové formáty

- Postfix – vylepšené parsování
- Checkpoint – přidána podpora pro nové formáty logování
- LOGmanager – vylepšeno parsování interních zpráv
- Windows DHCP – doplněna lookup tabulka s informací o důvodu nepřidělení IP adresy.
- HP Aruba – wireless tag byl odebrán z parseru a přesunut do klasifikace, tento parser nově podporuje i ne-wireless HP Aruba zařízení.
- Flowmon – doplněny překlady severity
- Firepower – drobné opravy a optimalizace
- Windows – drobné opravy a optimalizace

5.1.5 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

5.1.6 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

5.1.7 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

6 Opravené chyby

6.1.1 Verze 3.8.0

- Prohledávání záznamů webového rozhraní v konfiguračních formulářích občas nefungovalo správně.
- Některé automaticky generované reporty nebyly včas dokončeny.
- O365 zdroj nepracoval přes systémovou proxy.
- Webové rozhraní LOGmanageru nezobrazovalo informace o iLO/iDrac rozhraní.
- Decode CEF Blockly blok nepodporoval poslední verzi standardu CEF. Některá CEF pole využívající nových vlastností CEF formátu proto nebyla správně zpracována.

6.1.2 Verze 3.7.0

- O365 komponenta nerespektovala nastavení externího proxy serveru a připojovala se přímo do internetu.
- Opraveny názvy lite parserů v lookup tabulce tak, aby souhlasily s nastavením v klasifikátorech.
- Změněna architektura interního frontování, zrychlení systému v případě, kdy používá fronty.
- Na systémech s integrovaným LOGmanager Workload akcelerátorem nemuselo za specifických situací dojít k odmazání nejstarších dat, což způsobilo alertování administrátora o chybovém stavu systému (nová data se stále v pořádku ukládala).
- Opravena chyba, kdy parsovací proces mohl výrazně spamovat log interními chybami.
- Opraveno tlačítko shutdown v bootmenu.
- Opraveno oprávnění pro O365, nebylo možné oprávnění přidělit žádné skupině.

6.1.3 Verze 3.6.2

- Opraveny matematické operace uvnitř kontextů.

6.1.4 Verze 3.6.1

- Aktualizován kernel, který opravuje velmi pomalou komunikaci s řadičem disků na některých HP serverech.
- Oprava LEEF decode bloku, který nově umí dekódovat dle kompletní specifikace LEEF formátu.
- Oprava exportu zálohy na externí SMB server, za určitých podmínek mohlo dojít k nakopírování nekompletní zálohy.
- Vylepšeno zobrazení NTP status stránky o další možné stavy NTP služby.
- Dočasně odstraněna nefunkční konfigurace trunk (link agregace) interface z CLI LM.
- Upozornění – události zpracované uživatelským parserem, které v sobě neměly umístěný return blok, nebyly odeslány na další zpracování v alertech. Nově je veškerý provoz odesílán na zpracování v alertech.

- Opravena memory leak chyba procesů starající se o běh DB, exporty, zavírání/otevírání indexů apod. Chyba způsobovala, že procesy mohly spotřebovat násobně více paměti, než bylo navrženo. Důsledkem mohlo být zpomalení celého systému.

6.1.5 Verze 3.5.2

- Oprava možného pádu služeb celého systému LOGmanager. Tento stav se podařilo replikovat pouze na LMDemo boxech, ale preventivně vydáváme opravu pro všechny LOGmanager modely.
- Oprava LEEFv2 dekodéru.
- Oprava SQL komponenty – za určitých okolností mohlo dojít k pozastavení čtení z tabulek používajících časové razítko v „datetime“ formátu. (Formát „datetime2” je bez problémů)

6.1.6 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).

6.1.7 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.

6.1.8 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.

7 Známé chyby

7.1.1 Verze 3.2.4 až 3.8.0

- Problém: Editace databázového oprávnění občas nenačte bloky.
- Workaround: Znovu načíst stránku.

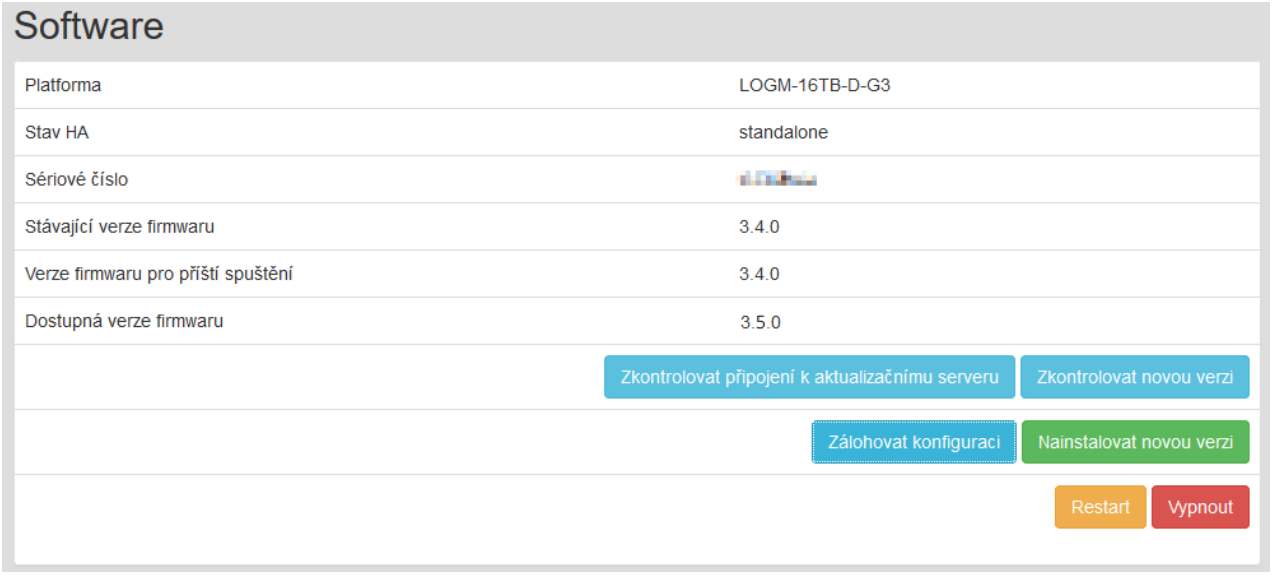
- Problém: Editace databázového oprávnění občas nezobrazí přeložené názvy tagů.
- Workaround: Přepnout na xml zobrazení a zpět, tagy se přeloží.

- Problém: Po editaci bloku (v klasifikaci, alertu, parsovacím pravidle) nelze změny uložit. Systém hlásí při pokusu o uložení chybu.
- Workaround: Zkontrolujte, zda jste při modifikaci bloku „add tag“ nevytvářel/a omylem nový, ale současně již existující tag stejného jména. Pokud ano, změňte tag na libovolný jiný a blok uložte.

8 Postup aktualizace

UPOZORNĚNÍ: Release 3.8.0 podporuje postupný upgrade clusteru. Aktualizaci clusteru je nutné provést instalací nového SW na oba boxy a první restartovat Cluster Master. Po doběhnutí restartu Cluster Master do provozního stavu lze následně restartovat Cluster Slave.

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 **3.8.0.**
- 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 **3.8.0.**
- 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.