LOGmanager release notes verze 3.1.1

Verze:	3.1.1	**Datum:**	16.08.2018

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 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)

2.1.2 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 Poznámky k vydání

3.1.1 Verze 3.1.1 - 16.8.2018

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.

3.1.2 Verze 3.0.1 - 30.4.2018

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 3.1.1

- 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.

4.1.2 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 3.1.1

- 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%.

5.1.2 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 3.1.1

- 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.

6.1.2 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 3.1.1

- 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.

- Problém:
  - Výpadek cluster master může za určitých okolností způsobit zahlcení cluster slave.
- Workaround:
  - Systém posílá maily s informací o případných problémech. Jakmile zjistíte výpadek cluster master, proveďte na cluster slave manuální rozpojení clusteru. Po zprovoznění rozbitého boxu proveďte znovu propojení do clusteru, jako cluster master ustanovte box, na kterém jsou uloženy všechny denní indexy.

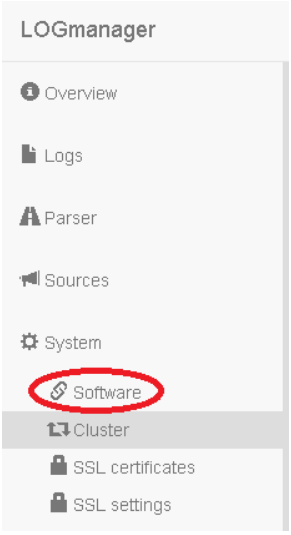
- Problém:
  - Při práci v dashboardech, při prohledávání na delším časovém úseku, se prvních 7 dní vykreslí rychle, pak se vykreslování zpomalí.
- Workaround:
  - Trpělivost. Vzhledem k omezeným zdrojům appliance je pouze posledních 8 denních indexů trvale otevřeno v paměti. Práce s uzavřeným denním indexem vyžaduje nejprve jeho otevření, a tudíž je přístup k datům starším než 7 dní o něco pomalejší. Zrychlení práce v dashboardu lze dosáhnout minimalizováním řádku s histogramem (collapse raw), pokud jej při daném prohledání nepotřebujete vizualizovat. Optimalizace připravujeme.

- Problém:
  - V menu Přehled / Stav databáze mohou být zobrazeny starší denní indexy s nulovou velikostí.
- Workaround:
  - Pokud po upgrade na software 3.1.1 daný denní index ještě nebyl otevřen, systém nezná jeho přesnou velikost a zobrazuje 0 B. Po prohledávání daného indexu v dashboardech, nebo po jeho manuálním otevření se velikost automaticky doplní.

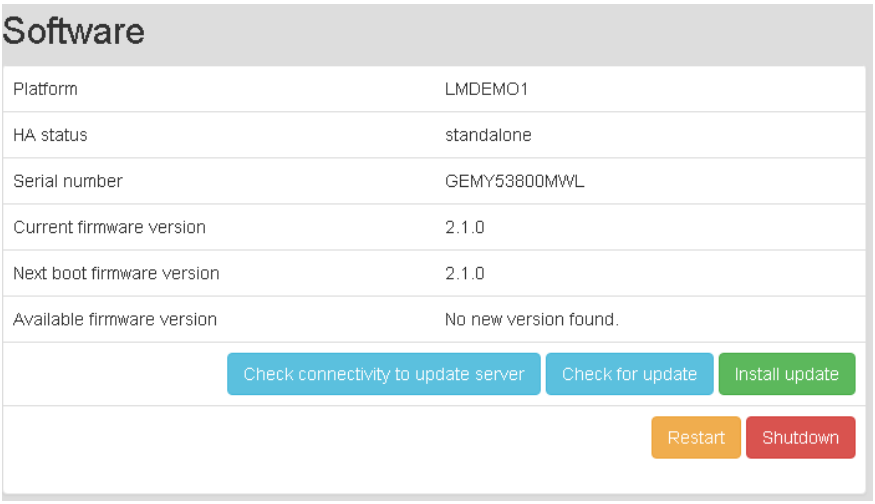
8 Postup aktualizace

UPOZORNĚNÍ: Release 3.1.1 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 Settings > Software



Otevře se stránka s informací o nainstalovaném software



Postup upgrade:

- Klikněte na tlačítko „Check for update“.
- Zobrazí se dostupná verze **3.1.1.**
- Klikněte na tlačítko Install update.
- Po opětovném načtení stránky se v next boot firmware zobrazí **3.1.1.**
- 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.