LOGmanager release notes verze 2.6.2

Verze:	2.6.2	**Datum:**	15.01 2018

1 Obsah

2 Úvod

Tento dokument popisuje následující souhrn vylepšení, informace k podpoře, instalační instrukce, seznam opravených chyb a popis nových funkcí.

2.1 Podporované modely

2.1.1 Verze 2.5.1, 2.6.1, 2.6.2

Podpora následujících modelů:

- LM-36 (2U HP gen8, 12x 3TB HDD, 64GB RAM, 2x6core CPU)
- LM-36B (2U HP gen9, 12x 3TB HDD, 64GB RAM, 2x8core CPU)
- LM-12B (1U HP 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-16TB-D (1U Dell R430, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-H (2U HP gen9, 12x 10TB HDD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-H (2U HP gen9, 12x 4TB HDD, 64GB RAM, 2x10core CPU)
- LOGM-16TB-H (1U HP gen9, 4x 4TB HDD, 64GB RAM, 1x10core CPU)

2.1.2 Verze 2.3.0, 2.4.0

Podpora následujících modelů:

- LM-36 (2U HP gen8, 12x 3TB HDD, 64GB RAM, 2x6core CPU)
- LM-36B (2U HP gen9, 12x 3TB HDD, 64GB RAM, 2x8core CPU)
- LM-12B (1U HP gen, 4x 3TB HDD, 64GB RAM, 1x8core CPU)
- LM-DEMO1 (Mini ITX Intel NUC, 1x 500GB SSD, 16GB RAM, 1x2core 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-16TB-H (1U HP gen9, 4x 4TB HDD, 64GB RAM, 1x10core CPU)

2.1.3 Verze 2.0.0, 2.1.0, 2.2.0

Podpora následujících modelů:

- LM-36 (2U HP gen8, 12x 3TB HDD, 64GB RAM, 2x6core CPU)
- LM-36B (2U HP gen9, 12x 3TB HDD, 64GB RAM, 2x8core CPU)
- LM-12B (1U HP gen, 4x 3TB HDD, 64GB RAM, 1x8core CPU)
- LM-DEMO1 (Mini ITX Intel NUC, 1x 500GB SSD, 16GB RAM, 1x2core 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)

3 Poznámky k vydání

3.1.1 Verze 2.6.2 - 15.1.2018

Opravná verze pro 2 méně závažné chyby. Tato verze nepřidává nové funkce ani parsery.

3.1.2 Verze 2.6.1 - 16.12.2017

Kompletně přepracován parsovací engine, sníženy nároky na paměť a zvýšen výkon parserů.
Přidána podpora pro přeposílání na více externích syslog serverů a filtraci přeposílaných zpráv.
Změněn název pole alertu z msg.alert@name na meta.alert.

3.1.3 Verze 2.5.1 - 15.9.2017

Aktualizace jádra a platformy operačního systému. Optimalizace konfigurace systému.
Systém nově stahuje aktualizace pouze ze serveru: up.logmanager.cz, pokud máte na firewallu pravidla limitující komunikaci LOGmanageru do internetu, prosím zkontrolujte, zda je up.logmanager.cz povolen.
Výrazně přepracovány parsery pro CEF, LEEF a fortigate viz poznámky níže.
Nová verze systému vyžaduje aktualizaci komponent (SQL, VMWARE, CHECKPOINT), aktualizace se provede automaticky během deseti minut po startu systému do nové verze. Systém musí mít po tuto dobu přístup k aktualizačnímu serveru.

3.1.4 Verze 2.4.0 - 21.4.2017

Opravy závažných memory leak, opravy interního monitorovacího systému.
Doporučujeme provést aktualizaci na tuto verzi v nejbližším možném termínu.

3.1.5 Verze 2.3.0 - 31.1.2017

Drobné opravy, nové parsery.
Vylepšení parsovacího engine, zvýšení výkonu.

3.1.6 Verze 2.2.0 - 17.1.2017

Přidána podpora pro přeposílání rozparsovaných JSON zpráv na externí syslog server.
Drobné opravy, nové parsery.

3.1.7 Verze 2.1.0 - 23.11.2016

Vrácena podpora pro řízení databázového oprávnění.
Přidána podpora pro LOGmanager forwardery.

3.1.8 Verze 2.0.1 - 7.10.2016

Drobné opravy, nové parsery.

3.1.9 Verze 2.0.0 - 14.9.2016

Přepsána velká část celého systému. Mezi hlavní novinky patří nový parsovací engine, který je plně uživatelsky nastavitelný. Uživatelsky je možné vytvářet a modifikovat parsery pro různé zdroje událostí.
Z důvodů možnosti definice vlastních parserů byl kompletně změněn formát uložených dat.
Byla vypnuta autodetekce typu přijímaných zpráv, nově je nutné jednotlivé zdrojové zařízení/subnety/obsah zprávy definovat v tzv. classifierech. Pro běžné používané zdroje dat je v systému předpřipravena konfigurace, do které stačí doplnit IP subnety.
Upozornění: Pro tento release je dočasně odstraněna možnost definovat práva přístupu k databázi, uživatelské oprávnění bude kompletně přepracováno ve verzi 2.1.x

4 Nové funkce

4.1.1 Verze 2.6.1

- Přidána podpora pro přeposílání událostí na více externích syslog serverů.
- Alerty nově umožnují definovat akci na přeposlání zprávy na externí syslog server (filtrace událostí, které budou přeposlány na externí syslog server).
- Změněn název pole v kterém je uložen název alertu. Zrušeno pole msg.alert@name, které bylo nahrazeno polem meta.alert. Nově je do pole meta.alert vložen název všech alertů, které zprávu označily.
- Přepracován parsovací engine, o 60 % menší nároky na paměť, parsování zpráv je o zhruba 20 % rychlejší (nejedná se o navýšení výkonu celého zařízení).
    - Nově se při testech parserů vrací zpět interní stavy chybových zpráv (pokusy o nastavení neexistujících proměnných apod.).
    - Při použití regulérních výrazů nově parsovací engine automaticky vytváří všechny názvy polí, které byly zadány (v původní implementaci se názvy polí nevytvořily, pokud byla hodnota prázdná).
- Reporty – do PDF se nově přidává hlavička LOGmanager s informací o názvu reportu a popisem reportu.
- SQL komponenta nově loguje informace o úspěšném připojení do databáze.

4.1.2 Verze 2.5.1

- Přidána podpora pro příjem událostí syslog protokolem na portech 51000 až 51100, TCP i UDP. Nově je možné provést klasifikaci a následné parsování událostí na základě informace o tom, na který port událost dorazila.
- Přepracovaná komponenta pro čtení dat z SQL databází:
    - Přidána podpora pro čtení dat z PostgreSQL,
    - Přidána podpora pro názvy SQL databází a tabulek obsahující speciální znaky (tečky, české znaky, mezery apod.).
    - Vylepšeny chybové hlášky.
- Nová verze komponenty pro VMware:
    - Aktualizace VMware SDK, optimalizace.
    - Vylepšeny chybové hlášky.
- Nová verze komponenty pro Check Point:
    - Aktualizace Check Point OPSEC SDK, optimalizace.
    - Přidána podpora pro připojení OPSEC protokolem na Check Point verze R80.x
    - Vylepšeny chybové hlášky.
- Přidána podpora pro XL verze LOGmanager.
- Aktualizace jádra a platformy operačního systému.
- Úprava konfigurace komprimace webových dotazů.
- Optimalizace konfigurace RAID řadiče.
- Podmínky v Alertech/parserech/klasifikaci nově respektují zapojení blockly a dle toho vytvářejí příslušné závorky. Původně byly bloky vyhodnocovány bez závorek. Nově jsou závorky automaticky přidávány dle zapojení v blocích. Příklad: if False and (False or True), původně bylo napsáno jako if False and False or True.

- Parsery jsou nově odolnější proti Regular Expressions catastrophic Backtracking (viz http://www.regular-expressions.info/catastrophic.html).
- Zabudované dashboardy nově prohledávají posledních 12 hodin (původně nastaveno na 24 hodin).

4.1.3 Verze 2.4.0

- Databázové skupiny nově podporují vytvářet pravidla s negací.
- Přidána podpora pro zálohování konfigurace LOGmanager serveru.
- Přidána podpora pro čtení SQL zdrojů z Oracle databáze.
- Přidána podpora pro připravovanou verzi Windows agenta 3.x.
- Interní diskové fronty událostí čekajících na zpracování jsou nově ukládány v komprimované podobě. Upozornění: Při nárůstu velikosti diskové fronty příchozích událostí na více než 10GB, je nově zasláno emailové upozornění na správce systému. V případě použití diskových front se výrazně zpomaluje rychlost vkládání nových událostí do databáze a část výkonu diskového subsystému je použita na práci s frontou událostí. V momentě, kdy velikost fronty událostí překročí hranici 50GB začne LOGmanager automaticky zahazovat přijímané události.
    - V normálním objemu provozu se diskové fronty příchozích událostí nevyužívají. Disková fronta je používána pouze ve chvílích, kdy je na LOGmanager zaslán nárazově výrazně větší objem příchozích událostí, než je systém v reálném čase schopen zpracovat a uložit do databáze.

4.1.4 Verze 2.3.0

- Aktualizován seznam výrobců MAC adres.
- Přidána podpora pro použití schéma u čtení z Microsoft SQL databáze.
- Klasifikátory jsou nově pro příjem zpráv seřazeny dle abecedy. Jakmile zpráva neskončí v klasifikátoru, prochází dalším klasifikátorem, který je dle abecedy v pořadí. Pořadí průchodu klasifikátory je abecední.
  Toto si vyžaduje drobné vysvětlení: *Pokud máte více klasifikátorů pro stejný zdroj dat (například Syslog nebo Windows) a v prvním klasifikátoru dle abecedního pořadí jména klasifikátoru nedojde událost k výstupovému pravidlu „Pass to Parser“, systém událost nezahodí. Pokračuje v zpracovávání události v dalším klasifikátoru pro daný zdroj dat podle abecedy. Pokud nevytváříte klasifikátory sami, ale jen upravujete existující klasifikátory, tak tato funkce pro Vás není zajímavá.*
- Drobné optimalizace parsovacího engine – zvýšení výkonu parsování o 50-100% dle druhu zpracovávané zprávy. Poznámka – nejedná se o zvýšení výkonnosti databáze ani celkového množství událostí za sekundu.

4.1.5 Verze 2.2.0

- Přidána podpora pro přeposílání událostí na nadřazený syslog server.
- Přidána podpora pro příjem a parsování událostí v LEEF formátu.
- Přidáno tlačítko na otestování spojení s aktualizačním serverem (System > Software).
- Vylepšená konfigurace webserveru:
    - Povolené je pouze TLSv1.2 šifrování spojení.
    - Přidány HSTS bezpečnostní hlavičky.
- Dashboardy:
    - Zvětšena pole pro zadávání názvu polí.

    - Vylepšen dashboard pro zobrazování práce s Windows soubory, zobrazování alertů, postfix/sendmail a Windows Logons.
- U blockly byla vypnuta funkce zoom na kolečku myši.

4.1.6 Verze 2.1.0

- Databázové oprávnění:
    - Přidána podpora pro definice skupin omezující přístup k databázi. Přístup je řízen na základě tagů.
- Přidána podpora pro připojení LOGmanager forwarder.
- Přepracován systém interních front zpráv:
    - Rozdělení front na dvě úrovně (raw při příjmu a před uložením události do databáze).
    - Pro frontu se primárně využívá operační paměť. Při velké zátěži začne systém automaticky odkládat události do dočasných souborů na pevném disku, které zpracuje při snížené zátěži.

4.1.7 Verze 2.0.0

- Vlastní parsery:
    - Je nutné definovat pravidla pro klasifikaci dat a jejich následné parsování (classifier).
    - Classifiery umožňují používat například IP prefix listy, část hostname atd. pro jednodušší konfiguraci celého systému.
    - Parsery je možné uživatelsky vytvářet a definovat jejich chování.
    - Definice parserů umožňuje vložit testovací události, které jsou živě parsovány dle aktuální definice parseru.
    - Parsery umožnují přetypovat data na IP adresu (automatické doplnění GEO IP, DNS PTR apod.) na MAC adresu (automatické přeformátování a doplnění informace o výrobci MAC adresy), INT a FLOAT (přetypování na číslo).
- Změněna struktury uložených dat:
    - Přidány meta informace.
    - Pole msg - obsahuje uživatelsky definované pole (rozparsovaná data).
    - Pole raw - obsahuje originální zprávu v nezměněné podobě.
    - Raw_offset – obsahuje informaci, kde v raw zprávě začínají data pro parser.
- Upraveny jednotlivé komponenty pro práci s novým formátem dat:
    - Checkpoint
    - Vmware
    - SQL
    - SAP
- Úpravy GUI pro lepší přehlednost a ovládání:
    - Do zobrazované URL byla přidána UID editovaného záznamu.
    - Stránky se po kliknutí Save nevrací na přehled, ale zobrazení zůstane na editovaném záznamu.
    - Přidána možnost uložit kopii editovaného objektu (Parsery, Classifiery, IP prefixy apod.).
    - Barevné zvýraznění řádků po najetí myši.
- Nová verze alertovacího systému, alerty nově umožnují velmi detailní definici pravidel pro zaslání alertu.
- Podpora lookup tabulek v parserech a alertech.
- Přidána podpora pro definici proxy serveru pro stahování aktualizací systému.

- Přidána kompletní podpora pro nahrávání a správu vlastních SSL certifikátů.
- Optimalizace JavaScript, výrazně rychlejší odezva GUI.
- Přidána podpora pro šifrované odesílání zpráv z Windows agentů (nutné vytvořit druhý SRV záznam _logmanager-ssl v DNS! Podrobný návod je v dokumentaci).
- Windows agent umožnuje zapnout ověření validity certifikátu LOGmanager serveru.
- Úprava minimální délky hesla lokálních uživatelů na 10 znaků.

5 Nové parsery:

5.1.1 Verze 2.6.1

- Nové parsery:
  - Samba audit log
- Aktualizované parsery:
  - CEF
    - Parser neumožňoval parsovat zprávy, které obsahovaly znak dolaru.
  - Kaspersky
  - Aruba – přidána podpora pro instant AP
  - HP Comware
  - Kerio connect
  - Sophos
  - Ironport
  - Trapeeze
  - Freeradius
  - Postfix
  - Apache JSON

5.1.2 Verze 2.5.1

- Nové parsery:
  - Amavis
  - Exchange mail log
  - Synology NAS DSM
- Aktualizované parsery:
  - CEF
    - Parsery nově překládají názvy polí dle doporučení LOGmanager (viz. https://doc.logmanager.cz/manual/lm/cs/standardized-variable-names.html) Existující vlastní parsery je nutné upravit na nové chování parsovacího engine.
  - Leef
    - Parsery nově překládají názvy polí dle doporučení LOGmanager (viz. https://doc.logmanager.cz/manual/lm/cs/standardized-variable-names.html) Existující vlastní parsery je nutné upravit na nové chování parsovacího engine.
  - FortiGate
    - Parser byl kompletně přepracován, nově nejsou do parsování zahrnuta duplicitní pole: dstcountry, srccountry, level, date, time. Všechna tato pole jsou již uložena v meta informacích.
  - Cisco ASA
  - Trapeeze
  - Checkpoint
  - OpenSSH
  - Windows file access
  - HP Procurve
  - HP Comware
  - Kerio connect

- Cisco IOS

5.1.3 Verze 2.4.0

- V této verzi byly kompletně odstraněny staré verze parserů, všechny parsery jsou již nově přepracovány do nového formátu.
- Seznam starých parserů aktualizovaných do nového formátu:
  - Trapeze
  - Kernun
  - Gama-web
  - Edirectory
  - AV Eset
  - Avast
  - Mysql
  - MicrosoftSQL
- Nové parsery:
  - Json – jednoduchý JSON parser, který provádí standardizaci běžně používaných polí.
  - Iron Port
  - Extreme networks
- Aktualizované parsery:
  - Juniper
  - ISC DHCP server
  - Kerio connect
  - Checkpoint
  - Flowmon
  - SQL
  - SonicOS

5.1.4 Verze 2.3.0

- Úprava zabudované klasifikační šablony pro Syslog – rozdělení do třech provázaných šablon pro lepší přehlednost. Tyto klasifikační šablony jsou seřazeny v následujícím pořadí:
  1) Syslog-template-IP
  2) Syslog-template-program_name
  3) Syslog-template-guessing

- Nové parsery:
  - Discard – speciální parser, který přijatá data zahodí.
- Přepracované parsery:
  - Apache Tomcat
  - Cisco ASA

5.1.5 Verze 2.2.0

- Nové parsery:
  - Dell iDrac
  - Interní LOGmanager události
  - Mikrotik
  - Cisco FirePOWER

    - Palo Alto NGFW
    - Windows file access log
- Přepracované parsery se standardizovanými názvy políček:
    - SAP
    - Kaspersky antivirus
    - FortiAuthenticator
    - Brocade SAN
    - MS SharePoint
    - Force 10
    - ISC DHCP server
    - ISC Bind DNS server
    - Postfix
    - Windows firewall

5.1.6 Verze 2.1.0

- Přepracované parsery se standardizovanými názvy políček:
    - Kerio Connect
    - MySQL Windows/Linux audit log
    - UBNT rocket
    - UBNT Unifi
    - Dropbear SSH server
    - SonicOS
    - Flowmon CEF
    - CEF

5.1.7 Verze 2.0.1

- Přepracované parsery se standardizovanými názvy políček:
    - Cisco SMB
    - Cisco WLC
    - FortiDDoS
    - Kerio Control
    - HP Procurve

5.1.8 Verze 2.0.0

- Přepracované parsery se standardizovanými názvy políček:
    - Aruba
    - Fortimail
    - Freeradius
    - JuniperSRX
    - Dell PowerConnect
    - Spamassasin
    - Apache log JSON format / Apache log
    - Microsoft IIS
    - Nginx
    - Checkpoint
    - FortiGate

- Kerio control
- OpenSSH
- Microsoft DHCP
- Shorewall
- Sophos
- VMware

6 Opravené chyby

6.1.1 Verze 2.6.2

- Export z tabulky do CSV selhal, pokud obsahoval pole meta.pole1@pole2 nebo msg.pole1@pole2 s nulovým obsahem.
- Testovací pole vytvářeného alertu neposkytovalo správný výsledek, pokud byl testovaný log z Windows Event Senderu (WES).

6.1.2 Verze 2.6.1

- Do bloku pro zpracování IP adres nebylo možné zadat IPv6 adresu.
- Opravena chyba generování reportů, pokud název reportu obsahoval mezeru, report nebyl odeslán.
- Opraven pád databáze na demo zařízení (P/N: LM-DEMO1), ke kterému docházelo z důvodu nedostatku operační paměti.
- LOGmanager Systém za určitých okolností zasílal emaily na neexistující doménu platform.sirwisa.cz. Emaily obsahovaly informaci o tom, že se nepovedlo přeložit hostname LOGmanager serveru. Toto bylo opraveno a byla provedena kontrola, že LOGmanager zasílá všechny varianty provozních a chybových stavů pouze na interní syslog. (LOGmanager systém nezasílá žádné informace o svém provozu na externí systémy).
- Opraven dashboard HP Spanning Tree log.
- Opraven dashboard CheckPoint audit log.
- SQL komponenta chybně logovala hostname SQL serveru do pole meta.src.ip.

6.1.3 Verze 2.5.1

- Opraveno exportování velkého množství událostí. Data jsou nově exportována v gzip formátu. Export má nově implementován limit na maximální počet exportovaných zpráv = maximálně 100 miliónů zpráv v jednom exportu.
- Opraveno řazení vygenerovaných reportů.
- Opraven interní monitoring stavu NTP serverů, nově přijde upozornění až ve chvíli, kdy jsou všechny NTP servery nefunkční.

6.1.4 Verze 2.4.0

- **Oprava zasílání systémových chyb, přidán alert na velikost fronty událostí čekající na zpracování.**
- Parsery:
    - **Oprava memory leak, který se projevoval při zpracování velkého množství velkých zpráv** (Více jak 80kB/zpráva)
    - Oprava bloku Create text.
    - Oprava bloku if in, při použití Windows.
    - Oprava bloku get last from list.
    - Oprava lookup tabulek při použití českých znaků.
    - Aktualizace integrovaného regexu pro zjišťování IPv4/IPv6 adresy.
    - Oprava bloku delete z proměnné message data.
- Opraven memory leak v RELP protokolu. Při velkém množství velkých zpráv začal proces příjmu RELP událostí konzumovat systémovou paměť.
- Opraven překlep v předmětu zasílaných reportů.

- Opraveno mazání nepoužitých Windows filtrů.

6.1.5 Verze 2.3.0

- Některé Windows systémy nepodporují připojení na TLS 1.2.
    - Úprava konfigurace webserveru, povolené jsou nyní šifry TLSv1.0, TLSv1.1 a TLSv1.2.
- Database groups – nebylo možné vybrat Forwarder name pro omezení přístupu k datům.

6.1.6 Verze 2.2.0

- Opraveno zasílání reportů.
- Opraveno chybové označení úspěšné instalace nové verze.
- Opraveno tlačítko test u LDAP skupin.
- Opravena chyba clusteringu – v některých případech nebylo možné vytvořit nový cluster.
- Oprava dashboardů, nebylo možné přidávat nové řádky.
- Oprava dashboardů, nebylo možné uložit dashboard se stejným názvem ve více databázových skupinách (při vytváření reportu je nově viditelný název databázové skupiny, se kterou bude report generován).
- Omezený uživatel si mohl upravit oprávnění.
- Opravena klasifikace Checkpoint.
- Opravena chyba v JS u klasifikátorů (v případě použití bloku „contain text“ se nebylo možné vrátit z XML editace do konfigurace bloků).
- Změněn limit pro odmazávání starých dat, pokud je k dispozici méně jak 35GB diskového prostoru, odmaže se nejstarší uložený den.

6.1.7 Verze 2.1.0

- Oprava RELP klasifikátoru. Zprávy odesílané na LOGmanager server pomocí RELP nebo RELP-SSL nebylo možné poslat do žádného parseru. Všechny zprávy odeslané pomocí syslogu, RELP nebo RELP-SSL jsou nově označovány jako syslog. Ke zprávám je navíc přidán příznak o tom, který protokol je přijmul (meta.src.dialect).
- Opravy parsovacího engine – práce s listy (funkce get first, get last) nefungovala správně.
- Oprava mapování pole „meta.tags“.

- Parser:
    - HP Aruba – parsování zpráv z Wireless IPS. Parser nově nevytváři hodnoty, které mají nulovou hodnotu.

6.1.8 Verze 2.0.1

- Opravena chyba v nastavení DNS PTR. Nebylo prováděno PTR pro privátní IP subnety.
- Opravena chyba v GUI konfiguraci checkpoint a vmware – nebylo možné přidávat tagy.
- Opravena chyba v syslog offsetu u Cisco zařízení.
- Oprava detekce názvu Cisco zařízení (hostname).
- Opravy dashboardů, přidán globální dashboard pro traffic log.

Parsery – opravy a přidání dalších typů zpráv pro parsování:

- Cisco IOS
- Cisco ASA
- Microsoft Windows
- HP Comware

6.1.9 Verze 2.0.0

- Opraven vzhled reportů. Výsledky reportu jsou již umístěny na správném místě.

7 Známé chyby

7.1.1 Verze 2.6.2, 2.6.1, 2.5.1, 2.4.0, 2.3.0, 2.2.0

- 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.

7.1.2 Verze 2.4.0, 2.3.0, 2.2.0

- Problém:
  - Při instalaci nové verze LOGmanageru může systém zobrazit modré informační pole s textem Error. Přesto instalace nové verze LOGmanageru proběhne úspěšně.
- Workaround:
  - Opraveno ve verzi 2.5.1
  - Ignorovat špatně definovanou chybovou hlášku.

8 Bezpečnostní upozornění

8.1.1 LOGmanager a zranitelnosti Meltdown/Spectre - 15.1.2018

3.ledna 2018 oznámila skupina bezpečnostních analytiků pod Google "Project Zero" popis nových vektorů útoků proti architektuře moderních procesorů. Zveřejněné techniky mohou vést k úniku informací čtením virtuální paměti. Technika nemůže vést k modifikování obsahu paměti, pouze k jejímu vcelku pomalému čtení. Více popisu k daným zranitelnostem naleznete na stránkách projektu Zero - link: https://googleprojectzero.blogspot.cz/2018/01/reading-privileged-memory-with-side.html nebo pod těmito CVE: CVE-2017-5753; CVE-2017-5715 a CVE-2017-5754.

Vývojáři naší společnosti provedli podrobnou analýzu a posouzení dopadů těchto zranitelností na rodinu produktů LOGmanager. Výsledkem analýzy je, že tyto zranitelnosti umožňují zneužití pouze na produktech, které umožňují spustit nedůvěryhodný kód. LOGmanager nepovoluje spuštění nedůvěryhodného kódu neoprávněným ani oprávněným uživatelem. Místa, kde lze vložit kód jsou ošetřena následovně: **Dashboardy** – důsledně ošetřeno proti vložení nedůvěryhodného kódu. **Blockly programy** integrované napříč LOGmanagerem – neobsahují programování časovačů, což je jedním z úspěšných předpokladů k volání daných zranitelností. **Integrovaná databáze** – neumožnuje spuštění uživatelských skriptů.

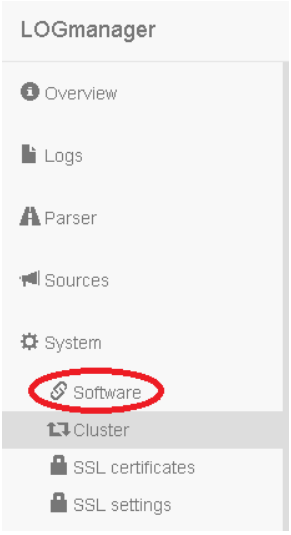
LOGmanager proto není zranitelný vektory útoků popsanými k 15.1.2018 v daných CVE.

I přes to, že LOGmanager není zranitelný, vývojáři přidají systémové opravy do kompoment LOGmanageru v příští verzi kódu. Podle našeho Security SDLC (Software Development Life Cycle) schématu trvale udržujeme LOGmanager produkty aktuální a analýzu možných zranitelností provádíme průběžně na vysoké úrovni. Produkty LOGmanager jsou vyvíjeny s ohledem na bezpečnost dat i vlastního systému (Privacy by design and by default).

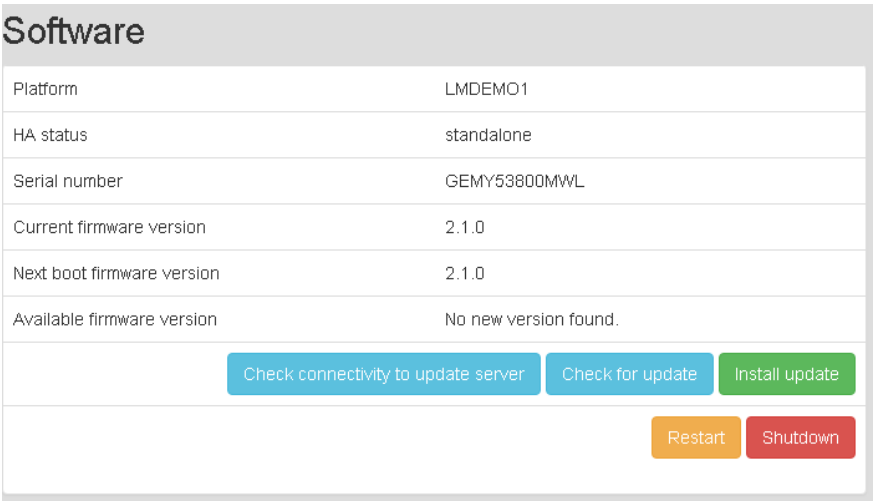
9 Postup aktualizace

UPOZORNĚNÍ: Release 2.6.2 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 **2.6.2.**
- Klikněte na tlačítko Install update.
- Po opětovném načtení stránky se v next boot firmware se zobrazí **2.6.2.**
- V posledním kroku stačí kliknout na Restart a systém se restartuje do nové verze.

9.1.1 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 30minut.

Konec dokumentu.