

# LOGmanager

- > Centrální úložiště logů
- > Dostupný SIEM



SPLŇUJE POŽADAVKY  
ZÁKONA O  
KYBERNETICKÉ  
BEZPEČNOSTI A GDPR

## LOGmanager release notes verze 3.2.2

<b>Verze:</b>	3.2.2	<b>Datum:</b>	5.12.2018
---------------	-------	---------------	-----------

**Omezující podmínky pro zveřejnění:**

*Tento dokument je chráněn autorskými právy a jako takový nesmí být bez předchozího souhlasu autora kopírován nebo předán třetí fyzické či právnické osobě.*

**Upozornění:**

*Všechny známky a názvy produktů uvedené v tomto materiálu jsou nebo mohou být registrované obchodní značky, obchodní značky nebo ochranné známky jejich vlastníků.*

---

[www.logmanager.cz](http://www.logmanager.cz)

**Sirwisa a.s.**

Zubatého 295/5, 150 00 Praha 5, IČ: 04667115, DIČ: CZ04667115

# 1 Obsah

LOGmanager release notes verze 3.2.2.....	1
2 Úvod .....	3
2.1 Podporované modely .....	3
2.1.1 Verze 3.2.2 .....	3
2.1.2 Verze 3.1.1 .....	3
2.1.3 Verze 3.0.1 .....	4
3 Poznámky k vydání .....	5
3.1.1 Verze 3.2.2.....	5
3.1.2 Verze 3.1.1.....	5
3.1.3 Verze 3.0.1.....	5
4 Nové funkce.....	6
4.1.1 Verze 3.2.2.....	6
4.1.2 Verze 3.1.1.....	7
4.1.3 Verze 3.0.1.....	7
5 Nové parsery: .....	8
5.1.1 Verze 3.2.2.....	8
5.1.2 Verze 3.1.1.....	8
5.1.3 Verze 3.0.1.....	8
6 Opravené chyby.....	9
6.1.1 Verze 3.2.2.....	9
6.1.2 Verze 3.1.1.....	10
6.1.3 Verze 3.0.1.....	10
7 Známé chyby.....	11
7.1.1 Verze 3.2.2.....	11
8 Postup aktualizace.....	12
8.1.1 Po restartu serveru.....	12

## 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 3.2.2 - 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)

#### 2.1.2 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)

### 2.1.3 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 Poznámky k vydání

### 3.1.1 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.

### 3.1.2 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.

### 3.1.3 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 3.2.2

- Přeprocovává funkce operace clusteru. Podrobné informace jsou v dokumentaci popisu clusteru: [naleznete zde](#).
- Přidána podpora pro zpětný import exportovaných událostí.
  - o LM si z externího SMB serveru stáhne vytvořenou zálohu a naimportuje jí zpět do systému.
  - o Všechna zpětně importovaná data jsou označena.
  - o Importovaná data nejsou ze systému automaticky odmazána, musí být ručně smazána z Database status stránky.
  - o Aktuálně je podporován pouze jeden současný import, pro import více dnů je nutné počkat na dobehnutí 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.

#### 4.1.2 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.
  - o 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.
  - o Každá akce vyhledávání v databázi nově vytváří zámky databáze. Zámky se vytváří pro systémové i uživatelské dotazy. Pokud na indexu existuje zámeček, není možné jej zavřít. Neobnovené zámky se automaticky uzavřou po 4 hodinách.
  - o Systém nově nedovolí otevřít a prohledat více dat, než je velikost dostupné operační paměti.
  - o 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 komprimovány 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.

#### 4.1.3 Verze 3.0.1

- Přidán korelátor událostí (upozornění s limitní hodnotou [alert with threshold] a korelace).
  - o Přidána definice kontextů a času jejich životnosti v rozsahu 60 až 900 sekund.
  - o Přidány nové vzory pro Alerty s kontexty.
- Parsery a alerty nově umožňují použití matematických operací.
- Parsery a alerty nově podporují dekodování URL (scheme, netloc, path, params, query, fragment, hostname, username).
- Přidán blok, který umožňuje 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 3.2.2

- 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.

### 5.1.2 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%.

### 5.1.3 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, icmpitype, log\_id, mastersrcmac, port, reqtype, sessionid, vip, wanin, wanout, wanoptapptype, countapp, countav, countweb, method, profilename, ref, ssl\_exempt).
  - 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 3.2.2

- 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.

### 6.1.2 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 certifikátu, 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.

### 6.1.3 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 kdokoli, 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

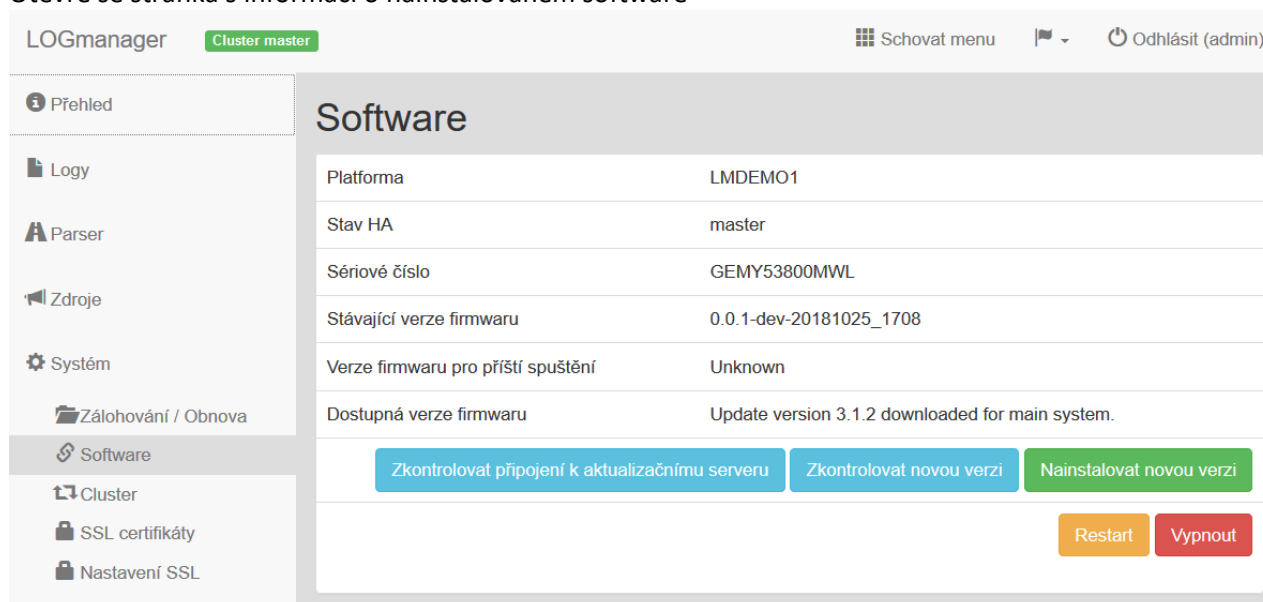
### 7.1.1 Verze 3.2.2

- 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:
  - 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 3.2.2 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 Systém > Software  
Otevře se stránka s informací o nainstalovaném software



The screenshot shows the LOGmanager web interface. The top navigation bar includes 'LOGmanager', 'Cluster master', 'Schovat menu', and 'Odhlásit (admin)'. The left sidebar contains navigation items: Přehled, Logy, Parser, Zdroje, Systém, Zálohování / Obnova, Software (highlighted), Cluster, SSL certifikáty, and Nastavení SSL. The main content area is titled 'Software' and contains a table with the following data:

Platforma	LMDEMO1
Stav HA	master
Sériové číslo	GEMY53800MWL
Stávající verze firmwaru	0.0.1-dev-20181025_1708
Verze firmwaru pro příští spuštění	Unknown
Dostupná verze firmwaru	Update version 3.1.2 downloaded for main system.

Below the table are three buttons: 'Zkontrolovat připojení k aktualizacímu serveru', 'Zkontrolovat novou verzi', and 'Nainstalovat novou verzi'. At the bottom right, there are 'Restart' and 'Vypnout' buttons.

Postup upgrade:

- Klikněte na tlačítko „Zkontrolovat novou verzi“.
- Zobrazí se dostupná verze **3.2.2**.
- Klikněte na tlačítko "Nainstalovat novou verzi".
- Po opětovném načtení stránky se v next boot firmware zobrazí **3.2.2**.
- 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.