Logmanager

# Logmanager – Poznámky k vydání – verze 3.9.9

| | | | |
|---|---|---|---|
| **Verze software:** | 3.9.9 | **Datum:** | 14. prosince 2022 |

# 1 Obsah

# 2 Úvod

Tento dokument popisuje následující souhrn vylepšení, informace k podpoře, instalační instrukce, seznam opravených chyb a popis nových funkcí od software verze 3.7.0 a výše. Pokud potřebujete podrobný popis pro verze software starší než 3.7.0, naleznete jej v dokumentaci Logmanager v menu „Poznámky k vydání“ nebo na uživatelském fóru Logmanager zde: https://forum.Logmanager.cz/viewforum.php?f=4

## 2.1 Podporované modely

### 2.1.1 Verze 3.9.9

- 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)
- LMDEMO-G3 (Asus MiniPC, 1x 500GB SSD, 32GB RAM, 1x8core CPU)
- LOGM-16TB-D-G4 (1U Dell R6515, 4x 4TB HDD, 64GB RAM, 1x16core CPU)
- LOGM-48TB-D-G4 (2U Dell R7525, 12x 4TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-96TB-D-G4 (2U Dell R7525, 12x 8TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-144TB-D-G4 (2U Dell R7525, 12x 12TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-192TB-D-G4 (2U Dell R7525, 12x 16TB HDD, 192GB RAM, 2x16core CPU)

# 3 Důležité poznámky k vydání

### 3.1.1 Verze 3.9.9

!!!
POZOR: Kompletní změna síťování v rámci Logmanager clusteru a mezi Logmanagerem a Logmanager Forwardery. Místo IPSEC je nově používán WireGuard protokol. Pro komunikaci v rámci clusteru je nutno povolit UDP port 51820. Pro komunikaci mezi Logmanagerem a Logmanager Forwarderem pak UDP port 51821.
!!!!

Sjednocení verzí operačního systému Logmanager napříč všemi podporovanými modely.
Podpora pro nasazení vylepšené viditelnosti do bezpečnostních událostí v prostředí Microsoft Windows díky možnosti nasazení a centralizované správě utility Microsoft Sysmon.
Přidána podpora pro běh více nodů v clusteru, nově jsou podporované až 4 nody.
Přidána podpora pro možnost automatického zpracování dat na všech nodech clusteru souběžně.
Přepracováno zobrazení stavu Logmanager Forwarderů.
Opravena chyba v komunikaci překladu názvu hostitelů (DNS PTR), která mohla za určitých okolností způsobit selhání řízení systémových úkolů. *Pokud byl Váš Logmanager touto chybou zasažen a byli jste technickou podporou vyzváni k vypnutí překladu názvu hostitelů (DNS PTR), po upgrade na tuto verzi software již můžete danou funkci zase aktivovat. Po aktivaci překladu není třeba restart.*

### 3.1.2 Verze 3.8.3 a 3.9.6

Tento build je primárně servisní a přináší opravy a drobné vylepšení. Upgrade z předchozí verze je nutný.
Oprava CVE-2022-24903 zranitelnosti Rsyslog.

### 3.1.3 Verze 3.8.2 a 3.9.5

Hlavní novinkou těchto verzí je nový systém pro sběr logů z Windows prostředí prostřednictvím nového Beat Agenta postaveného na open-source Elastic Beat (winlogBeat/fileBeat). 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.

Dle oznámení s verzí 3.6.1 byla ukončena podpora pro Checkpoint komponenty na stahování logů prostřednictvím OPSEC protokolu.

Verze 3.8.2 běží na původní verzi operačního systému.
Verze 3.9.5 běží na nové verzi operačního systému s vylepšenou podporou pro interní virtualizaci.
Poznámka: *Verze 3.8.2 a 3.9.5 jsou totožné co se funkčních vlastností týče, s rozdílem že verze 3.9.5 bude nabídnuta k instalaci pouze na nové verze hardware dle tabulky 2.1.2. V příští verzi software dojde k opětovnému sjednocení verzí pro všechny modely.*

### 3.1.4 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“.

# 4 Nové funkce

### 4.1.1 Verze 3.9.9

- Přepracován systém komunikace Logmanager clusteru a komunikace mezi Logmanagerem a Logmanager Forwardery z IPSEC na WireGuard. Systémy při prvním startu provedou automatickou migraci spojení z IPSEC na WireGuard. POZOR, je nutné aktualizovat všechny nody v clusteru!

  Pokud je v cestě mezi členy clusteru nebo mezi Logmanager Forwarderem a Logmanagerem Firewall, je nutné povolit prostup pro UDP port 51820 (cluster) a UDP port 51821 (Forwarder).
- Nově lze zapojit do Clusteru až 4 nody.
- Vypnuto TLS1.0 a TLS1.1. Nově je podporováno jen TLS1.2 a TLS1.3. Pokud stále používáte staršího Agenta pro sběr logů z Windows – Logmanager WES, již instalovaní WES Agenti budou fungovat nadále bez problémů, jelikož si z LM stáhnuli novější konfiguraci a používají TLS1.2. Nově nainstalovaní WES Agenti se k LM již nepřipojí bez manuálního zásahu do jejich konfigurace. V případě potřeby instalovat WES, kontaktujte technickou podporu na portále https://support.logmanager.cz. Doporučujeme však ukončit používání WES Agentů a přejít na Logmanager Beat Agenty.
- Nově jsou zobrazovány uložené hodnoty u zabudovaného obsahu (Regex substituce, Lookup tabulky, IP prefix listy).
- Možnost volby automatického rozložení zátěže zpracování příchozích zpráv na všech nodech v rámci clusteru.
- Přepracována stránka pro zobrazení stavu Forwarderů. Nově je zobrazen stav spojení s Forwarderem při načtení stránky a je zobrazena verze Forwarderu a je možné provádět aktualizace a restarty Logmanager Forwarderů z prostředí Logmanageru (od verze Forwarderu 3.9.x).
- Přidán odkaz na support portál na úvodní stránku uživatelského rozhraní.
- Příprava na nasazení Sysmon v rámci Beat Agenta pro obohacení vytvářených bezpečnostních událostí v Microsoft prostředí. Bližší detaily v online dokumentaci Logmanageru pod heslem „Sysmon“.
- O365 endpoint je nově možné směrovat na jakýkoliv node v clusteru nebo i skrz Logmanager Forwarder (od jeho verze 3.9.x).
- Vylepšená interní komunikace clusteru, cluster nově interně přeposílá požadavky na řídicí node. Nově se Beat a WES Agenti můžou dotazovat na svoji konfiguraci jakéhokoli nodu v clusteru.

- Beat Agent verze 1.0.42923:
  - Beat Agent nově obsahuje kompletní certificate chain v jeho podpisu. Nekompletní certificate chain mohl způsobovat problémy s aktualizací Agenta na systémech bez připojení k internetu.
  - Beat Agent obsahuje přepracovaný systém instalace. Nově je k dispozici jen jedna verze instalátoru (logmanager-orchestrator-service-installer.msi), která obsahuje možnost volby, zda Logmanager Beat Agent má podporovat vlastní automatickou aktualizaci či nikoliv.
  - Tato verze prozatím neobsahuje možnost instalace Sysmon. Pokud máte zájem o verzi umožňující centralizovanou instalaci a správu Sysmon, prosím kontaktujte technickou podporu Logmanageru na portále https://support.logmanager.cz.

- Nové dashboardy:
    - Sysmon overview
    - Sysmon file events
    - Sysmon process events
    - Sysmon registry events
    - Sysmon WMI events
    - Sysmon threat hunting
    - Vmware horizon
    - Secure anybox
    - Progress Kemp LoadMaster (pro systémové logy a logy loadbalanceru)
    - Progress Kemp LoadMaster WAF (pro web aplikační firewall)
- Opravené/vylepšené dashboardy:
    - Cisco config change
    - Progress Flowmon ADS
    - Vmware status change

### 4.1.2 Verze 3.8.3 a 3.9.6

- Přidaná možnost hromadného mazání Beat a WES Agentů z GUI Logmanager pomocí zaškrtávacích polí.
- Přepracovaný interní systém pro správu úloh.
- Přidán nový dashboard pro SecureAnyBox

### 4.1.3 Verze 3.8.2 a 3.9.5

- Nová verze **Beat Agenta** pro sběr logů z prostředí Microsoft Windows – s kompletní podporou minimálně na úrovni předchozího WES Agenta.
    - Původní verze sběru logů ponechána, pouze jméno doplněno o „legacy“.
    - Nové instalační 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.
    - Logmanager automaticky ořízne každou příchozí Beat souborovou zprávu, která přesáhne velikost 64000 bajtů. Každá oříznutá zpráva bude automaticky označená jako truncated. Více informací naleznete v dokumentaci.
    - 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 Agent -> Beat Agent: *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 Beat 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.*

Poznámka: *Nová verze Beat Agenta prozatím nepodporuje centrální konfiguraci a předávání logů prostřednictvím Logmanager Forwarderu. Podpora bude brzy přidána v nové verzi Forwarderu.*

- 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.
- Virtualizace interních komponent systému.
- 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

#### 4.1.4 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

# 5 Nové parsery:

### 5.1.1 Verze 3.9.9

- Nové parsery
  - Kemp LoadMaster
  - Sysmon
- Aktualizované parsery
  - FortiWeb
  - Beat-windows – přidána rozšířená podpora pro logy Windows Defender

### 5.1.2 Verze 3.8.3 a 3.9.6

- Nové parsery
  - VMware-horizon
  - Jivex
- Aktualizované parsery
  - FortiWeb
    - Pole „log_id“ přejmenováno na „attack_id“.
    - Přidána pole „msg_id“ a „signature_id“.
  - Fortigate
    - Oprava parseru, který za určitých okolností mohl vytvářet neplatná pole.
  - Fortigate-lite
    - Oprava parseru, který za určitých okolností mohl vytvářet neplatná pole.
  - Freeradius
    - Oprava parseru, který za určitých okolností mohl vytvářet neplatná pole.
  - Apache tomcat
    - Přidána podpora pro Beat Agenta.
  - Flowmon
    - Oprava parseru, který určitých okolností mohl vytvářet neplatné hodnoty, např. u „msg.vlan_id“.
  - OpenSSH
    - Oprava parseru, který určitých okolností mohl vytvářet neplatné hodnoty, např. u „msg.src_ip“.
  - Veeam
    - Přidána podpora pro Beat Agenta.
  - Beat-windows
    - Oprava parseru, který za určité konfigurace nesprávně parsoval některé logy a u polí přidával před hodnotu mezeru.
  - Qnap
    - Vylepšený parser a přidána podpora pro Qnap software verze 4.5.x
  - JSON
    - Přidána podpora pro fileBeat
  - Logmanager
    - Oprava parseru, který za určitých okolností mohl vytvářet neplatná pole.

### 5.1.3 Verze 3.8.2 a 3.9.5

- 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 informací ze status logů.
  - 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.

### 5.1.4 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.

# 6 Opravené chyby

### 6.1.1 Verze 3.9.9

- Opraveno možné selhání správce úloh (task-manager). Pokud jste během komunikace s technickou podporou Logmanageru při hlášení chyby selhání task manageru dostali instrukci, že do vydání nové verze je nutné vypnout překlad názvu hostitelů (DNS PTR), po aktualizaci na verzi 3.9.9 je možné tuto funkci opětovně zapnout.
- Logmanager Beat Agent verze 1.0.36635 se neumí automaticky aktualizovat. Bohužel chybou při sestavování Beat Agenta se dostala do distribuce verze Agenta, která neměla povolenou aktualizaci sebe sama. Pro následnou podporu automatické aktualizace Beat Agentů je nutné jednorázově provést aktualizaci manuálně nebo prostřednictvím MS AD GP.
- Opravena chyba, kdy obnovený index nemusel být správně uzamčen, a tím mohlo dojít k přerušení obnovení daného denního indexu.
- Změna konfigurace proxy se neprojevila ihned po nastavení, ale až po restartu Logmanageru.
- Oprava validace SMTP konfigurace a chybné textace české verze rozhraní.
- Optimalizace a zrychlení služby pro sběr dat z Beat Agentů.
- Změna konfigurace TLS certifikátů pro Syslog over TLS se neprojevila ihned, ale až po restartu.
- Opravena chyba, kdy nebylo možné obnovit exportovanou zálohu konfigurace kvůli nadměrné velikosti zálohy. Implementovány komprese interních konfigurací pro minimalizaci velikosti zálohy konfigurace.
- Omezení množství interních logů, které jsou uložené do databáze. Interní logy služeb se nově ukládají jen do debug logu přístupného v TSR.
- Oprava možného úniku SMB hesla pro backup index do notifikačního emailu pro správce systému při spadnutí task-manageru uprostřed zálohy. Doporučujeme změnit heslo pro dané uživatelské jméno použité pro zálohování denních indexů Logmanageru na externí SMB server.

### 6.1.2 Verze 3.8.3 a 3.9.6

- V interní komponentě Rsyslog došlo k záplatování zranitelnosti CVE-2022-24903.
- V instalačním balíčku MSI Beat Agenta je nově viditelná verze ve vlastnostech MSI souboru.
- Oprava DHCP šablony pro Beat Agenta.
- Testovací okno pro klasifikátory/parsery/alerty nesprávně procesovalo JSON zprávy.
- Logmanager Beat Agent neprováděl korektní změny DNS záznamů při jejich aktualizaci.
- Opravená funkce Sledování zdrojů, za specifických podmínek mohlo dojít k přetížení LM systému monitoringem zdrojů.
- Opraven Syslog output/syslog forwarding - ve specifickém scénáři mohlo dojít k neočekávanému chování.
- FileBeat konfigurace tagů je korektně escapovaná a je zasílána jako list, původně byla chybně zasílána jako jeden string i v případě více tagů.
- FileBeat opravena template pro monitoring DHCP logů.

### 6.1.3 Verze 3.8.2 a 3.9.5

- 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.

### 6.1.4 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.

# 7 Známé chyby

### 7.1.1 Verze 3.9.9

- Problém: Logmanager orchestrator agenti se neaktualizují na novější verzi.
- Popis: Chyba vydané špatné verze agenta, kdy do produkce uvolněna verze bez podpory sebeaktualizace. To bylo způsobeno nevhodně poskládaným build procesem, kdy v případě release došlu k race-condition a vydala se verze bez updateru. Tato chyba byla vyřešena změnou build procesu, takovým způsobem, že je vydávána jen jedna verze a podle parametrů se chová rozdílně.
- Workaround: Jelikož je v příštím LM release plánováno uvolnění sysmon, není nutné agenty hned ručně aktualizovat, protože sysmon bude vyžadovat opětovnou instalaci pomocí MSI. Do příští verze připravíme návody, jak tuto chybu odstranit.

- Problém: Oproti dokumentaci nelze použít zástupné symboly pro vytvoření pravidla pro sledování zdrojů (Source tracking)
- Workaround: Zatím je třeba manuálně vyspecifikovat všechny důležité hosty.

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

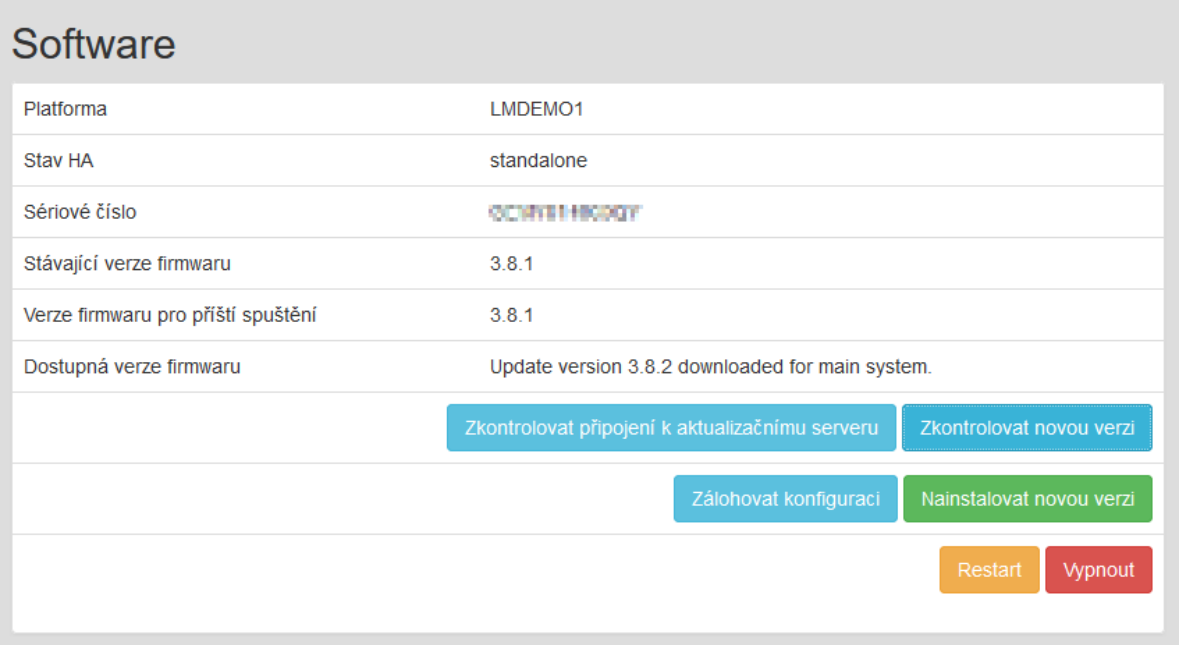
- Problém: Editace databázového oprávnění občas nezobrazí přeložené názvy tagů.
- Workaround: Přepnout na XML zobrazení a zpět, tagy se přeloží.

- 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 3.9.9 podporuje postupný upgrade clusteru. Aktualizaci clusteru je nutné provést instalací nového SW na všechny 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 **3.9.9**
- 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 3.9.9
- V posledním kroku stačí kliknout na Restart a systém se restartuje do nové verze.
- Po restartu systém konsoliduje a provádí kontrolu integrity databáze, automaticky aktualizuje použité komponenty a provádí všechny další potřebné kontroly. Toto může trvat až jednu hodinu. Prosíme, zachovejte trpělivost a nerestartujte během této doby systém znova.

### 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 déle.**

Konec dokumentu.