Microshop
intelligent systems
Sídlo: Pod Marjánkou 4, 169 00 Praha 6 Kancelář: Pod Marjánkou 4, 169 00 Praha 6
Zapsáno u Městského soudu v Praze obchodní rejstřík oddíl C, vložka 76081 IČO 26165031 DIČ CZ26165031

MS Custom LOG

Konfigurační příručka

Verze 2025_02

233 357 033-4 233 357 090 microshop@microshop.cz http://www.microshop.cz

1 Úvod

1.1 Účel dokumentu

Tento dokument slouží jako konfigurační příručka systému MS Custom LOG, který poskytuje jednotné a centralizované řešení pro sběr, správu, analýzu a archivaci logovacích dat a dalších událostí napříč IT infrastrukturou organizace. Je určen pro systémové administrátory a technické správce, kteří zajišťují konfiguraci systému, jeho přizpůsobení konkrétním potřebám a dohled nad jeho provozem.

Cílem dokumentu je poskytnout podrobný a srozumitelný návod k veškerým činnostem, které lze v systému konfigurovat prostřednictvím integrovaného webového rozhraní. Příručka popisuje způsob připojení různorodých zdrojů dat, tvorbu vlastních pravidel pro zpracování událostí, správu uživatelů a oprávnění, nastavení výstrah a notifikací, plánování záloh, propojení s externími nástroji i export a automatizaci reportů.

MS Custom LOG byl navržen s důrazem na bezpečnost, přehlednost a snadné ovládání bez nutnosti znalosti programovacích jazyků nebo skriptování. Všechny klíčové funkce systému – od vizualizace dat přes správu parserů až po správu přístupů – jsou dostupné prostřednictvím jednotné webové konzole.

Popisované funkcionality odpovídají aktuální verzi systému v době vydání dokumentu a budou průběžně aktualizovány dle vývoje a nasazení nových verzí.

Dokument je určen výhradně administrátorům systému. Pro běžné uživatele, kteří pracují pouze s výstupy systému (např. dashboardy a reporty), je určena samostatná uživatelská příručka.

1.2 Cílová skupina

Tato konfigurační příručka je určena především pro **systémové administrátory, správce IT infrastruktury a pracovníky odpovědné za bezpečnost informačních systémů**, kteří mají na starosti zavedení, správu, údržbu a bezpečný provoz systému MS Custom LOG.

Dokument slouží jako technický návod pro ty uživatele systému, kteří mají oprávnění provádět konfigurace v administrátorském rozhraní – zejména:

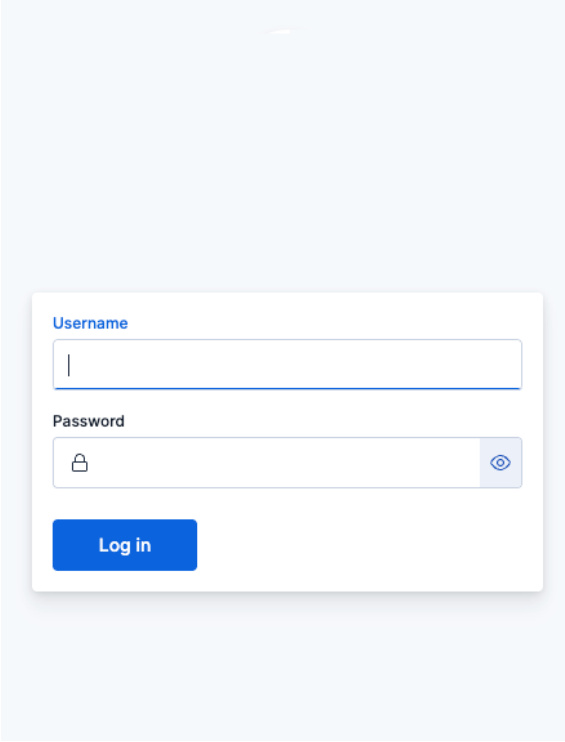
- připojovat nové zdroje logovacích dat a databází,
- nastavovat pravidla pro zpracování a tagování událostí,
- definovat parsery a přizpůsobovat výstupy systému,
- spravovat přístupová práva, uživatelské účty a role,
- nastavovat upozornění a plánovat notifikace,
- vytvářet a upravovat systémové dashboardy a reporty,
- provádět zálohování a obnovu systému,
- dohlížet na bezpečnost a soulad se standardy.

Příručka **není určena běžným koncovým uživatelům**, kteří systém využívají pouze ke sledování výstupů, přehledů nebo notifikací. Pro tyto účely je připravena samostatná uživatelská dokumentace s přehledem základních funkcí dostupných v režimu pouze pro čtení.

2 Přístup a správa uživatelů

2.1 Přístup do administrace

Administrátorské rozhraní systému **MS Custom LOG** je přístupné prostřednictvím zabezpečeného webového prohlížeče, a to na definované adrese (např. `https://<název-serveru>/`). Veškeré administrátorské funkce jsou součástí jednotného centrálního rozhraní, ve kterém se provádí jak konfigurace systému, tak jeho sledování a správa.



Přístup je chráněn **autentizací uživatele**. Systém podporuje následující jeden z následujících způsobů přihlášení:

- **Interní uživatelský účet** – spravovaný přímo v systému MS Custom LOG.
- **Externí adresářové služby** – připojení k LDAP nebo Microsoft Active Directory.

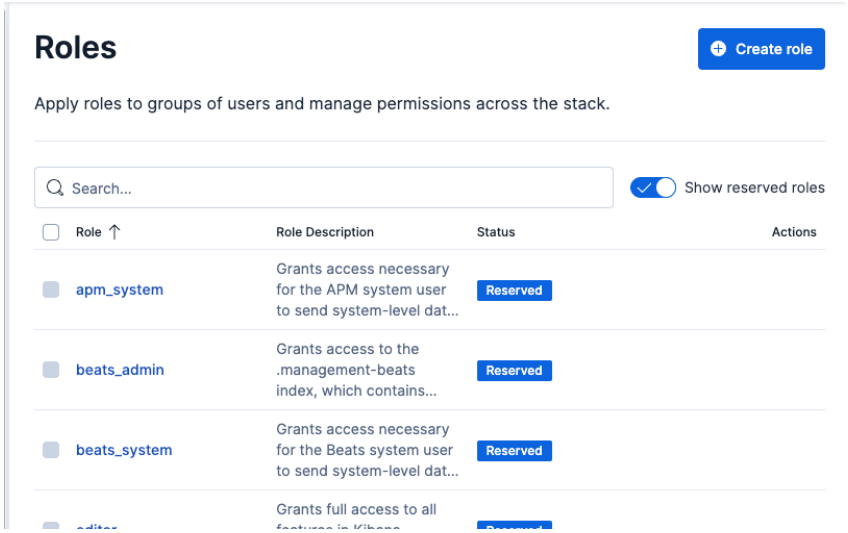
Uživatel musí být zařazen do jedné z rolí s oprávněním pro přístup do administrátorských částí rozhraní. Přístup je řízen na základě přiřazené role, která definuje oprávnění k jednotlivým modulům a datovým entitám v systému.

2.2 Správa uživatelských rolí

MS Custom LOG nabízí možnost **správy rolí a oprávnění** prostřednictvím uživatelského rozhraní. Role definují, **jaká oprávnění mají uživatelé** nad daty, dashboardy, indexy apod.

Ke správě rolí se dostanete v menu přes položky Management → Stack Management → Security → Roles.

Jeden uživatel může mít přiřazeno i více rolí.



Systém obsahuje spoustu předdefinovaných rolí včetně jejich popisu. Zde uvádíme některé z nich:

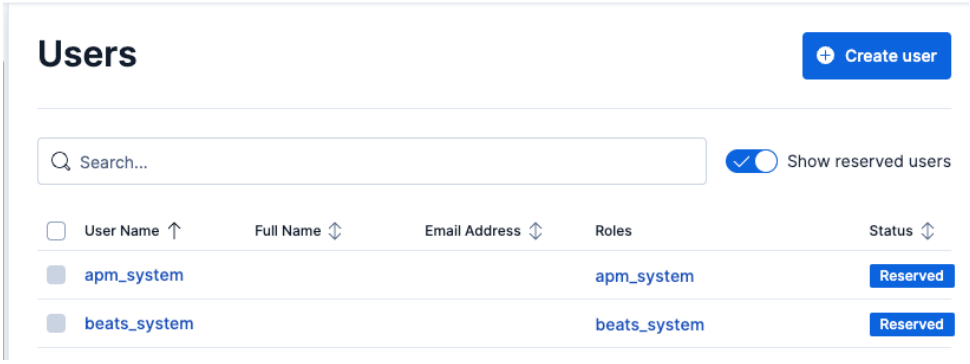
- superuser – neomezený přístup ke všem funkcím systému
- kibana_admin – plný přístup ke všem funkcím jednotného uživatelského rozhraní, ale ne k datům
- kibana_user – přístup k běžným uživatelským funkcí jednotného uživatelského rozhraní, ale ne k datům
- read_only – čtení všech logovacích dat
- logstash_admin – správa parserů dat
- beats_admin – správa vstupních zdrojů

Pokud by předdefinované role nestačily, je možné vytvořit vlastní role. U každé role se nastavuje k jakým datům má přístup a jaké moduly uživatelského rozhraní jsou přístupné.

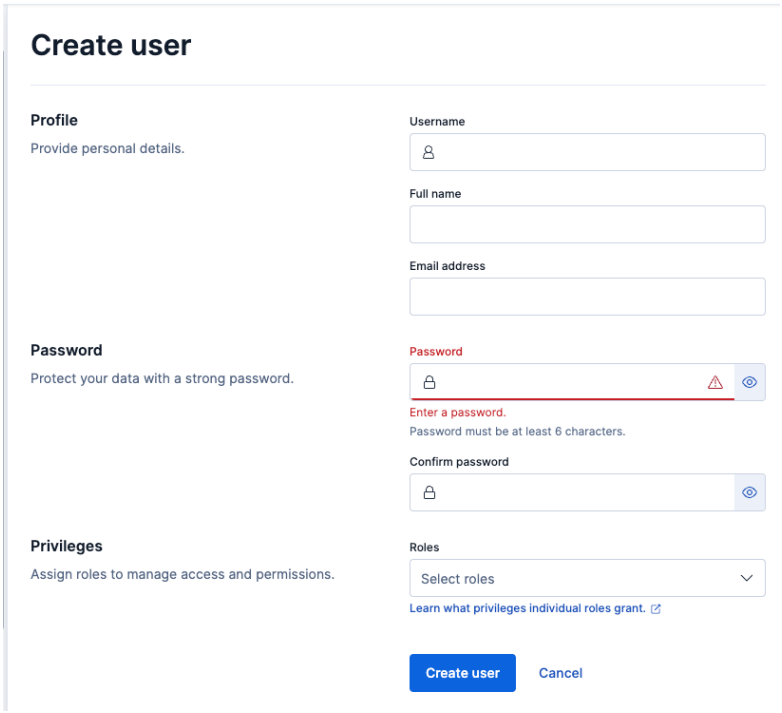
2.3 Správa uživatelů

Každý uživatel může mít přiřazené **jednu nebo více rolí**, které určují jeho oprávnění.

Ke správě uživatelských účtů se dostanete v menu přes položky Management → Stack Management → Security → Users.



Pomocí tlačítka Create user je možné vytvořit nové uživatele. Vyplníte všechny údaje a v Privileges vyberete jednu nebo více rolí.



Taktéž je možné vytvořené uživatele upravovat, deaktivovat, či mazat.

2.4 Napojení na LDAP nebo Active Directory

MS Custom LOG umožňuje pro přihlášení k systému využívat externí autentizační služby LDAP nebo Active Directory.

Ke správě integrace externích přihlašovacích služeb se dostanete v menu přes položky Management → Stack Management → Security → External.

Zde si vyberete zda chcete používat interní seznam uživatelů, LDAP nebo Active Directory.

V případě LDAP vyplníte:

- URL serveru – např ldap://ldapserver.local:389
- Bind DN – uživatel, pod kterým se přihlašuje k LDAP
- Bind password – heslo uživatele
- User search
  - Base dn – cesta kde se mají hledat uživatelské účty
  - Filter – filtr uživatelských účtů
- Group search – cesta kde se mají hledat skupiny
- Mapování LDAP groups na roles - nastavíme které role se přiřadí LDAP skupinám

V případě Active Directory:

- Domain – název domény Active Directory
- Mapování skupin Active Directory na role

3 Konfigurace vstupních zdrojů

3.1 Přehled podporovaných vstupních zdrojů

Systém **MS Custom LOG** podporuje široké spektrum vstupních formátů a protokolů, které umožňují flexibilní a škálovatelný sběr logovacích dat z různorodých systémů, zařízení a databází. Cílem je umožnit centralizaci všech relevantních dat bez potřeby instalace dodatečného softwaru na cílových systémech.

Seznam podporovaných formátů:

Formát	Popis	Poznámka
RAW UDP	Surový datový tok přes UDP protokol.	**Neomezený počet** instancí současně.
RAW TCP	Surový datový tok přes TCP protokol.	**Neomezený počet** instancí současně.
Syslog	Standardní protokol pro přenos logovacích zpráv (RFC 3164, RFC 5424).	Podpora UDP i TCP.
RELP	Reliable Event Logging Protocol – spolehlivý přenos zpráv.	Vhodné pro kritické systémy.
CEF	Common Event Format používaný bezpečnostními nástroji (ArcSight).	Plná kompatibilita.
LEEF	Log Event Extended Format – formát společnosti IBM.	Podpora pro SIEM integrace.
JSON (RFC8259)	Strukturovaná data ve formátu JSON dle standardu RFC8259.	Doporučený formát pro moderní aplikace.
Office365	Přímé napojení na logovací rozhraní Microsoft 365.	Bez nutnosti externích konektorů.
Winlog	Logy z Windows Event Viewer.	Vyžaduje instalaci agenta.
Websocket	Příjem dat přes WebSocket API (např. IoT zařízení).	Real-time integrace.
SNMP	Protokol pro příjem trapů a dotazování síťových prvků.	Vhodné pro monitoring infrastruktury.
JDBC	Přímé dotazování databází (MSSQL, MySQL, Oracle, PostgreSQL).	Bez nutnosti instalace na databázové servery.

Všechny vstupy se konfigurují z jednotného webového rozhraní, bez nutnosti zásahu do backendu nebo konfigurace na úrovni OS. **Není omezen počet současně aktivních vstupů** – jejich správa je automatizovaná a škálovatelná.

3.2 Správa vstupních zdrojů

Ke správě vstupních se dostanete v menu přes položky Management → Stack Management → Data sources.

Na stránce Data sources se zobrazí tabulka všech aktuálně nakonfigurovaných vstupních zdrojů. U každého zdroje jsou uvedeny základní informace:

- Název zdroje
- Typ vstupu (např. Syslog, Winlog, JDBC)
- Poslední aktivita (čas posledního přijatého záznamu)

Tabulka je vybavena možnostmi filtrování, vyhledávání a stránkování.

Přidání nového zdroje provedeme v pravém horním rohu tabulky klikněte na tlačítko „+ Přidat nový zdroj“.

Vyberte typ vstupního formátu (např. RAW TCP, Syslog, JSON...).

Vyplňte požadované údaje:

- Název zdroje
- Port nebo přístupový bod
- Další údaje závislé na daném typu zdroje. Přímo na stránce je u každého zdroje popsáno jaké údaje jsou potřeba.

Uložte konfiguraci kliknutím na „Vytvořit“.

Nový zdroj se okamžitě aktivuje a zobrazí se v seznamu.

Pro úpravu existujícího zdroje klikněte u příslušného řádku v tabulce na ikonu „Upravit“. Můžete změnit konfiguraci a technické parametry.

Pro smazání zdroje použijte ikonu „Odstranit“. Systém vás požádá o potvrzení.

Pozor: Odstraněním zdroje dojde k ukončení příjmu dat z daného rozhraní. Historická data zůstanou v systému zachována.

3.3 Sběr z prostředí Microsoft

Sběr logovacích dat z prostředí Microsoft (operační systémy Windows Server a klientské stanice, služby Active Directory, Exchange, SharePoint, SQL Server, a cloudová služba Microsoft 365) je v systému MS Custom LOG řešen jako samostatný, plně podporovaný scénář s důrazem na **bezpečný přenos, centrální správu konfigurace a škálovatelnost bez licenčního omezení**. Tato podkapitola popisuje doporučené architektury sběru a způsob jejich nastavení.

Podporované způsoby sběru

Systém umožňuje sběr událostí z prostředí Microsoft třemi vzájemně doplňujícími se způsoby, které lze v rámci jedné instalace libovolně kombinovat podle topologie sítě a bezpečnostních požadavků:

- **Sběr prostřednictvím agenta** instalovaného na cílových strojích Windows (servery i klientské stanice). Agent zajišťuje příjem událostí z Windows Event Logu, souborových logů a vlastních zdrojů a jejich šifrovaný přenos do centrálního systému.

- **Bezagentový sběr z cloudových služeb Microsoft 365** prostřednictvím přímého napojení na rozhraní Management Activity API. Tento režim nevyžaduje žádnou další komponentu na straně zákazníka.

Systém **neomezuje počet připojených Windows agentů ani koncových stanic** předávajících data přes WEC. Licenční model je vázán pouze na příchozí objem dat (EPS / GB), nikoli na počet zdrojů. Připojení dalšího agenta ani změna jejich počtu nevyžaduje rozšíření licence.

Šifrovaný přenos a autentizace zdrojů

Veškerá komunikace mezi zdroji v prostředí Microsoft a systémem MS Custom LOG probíhá výhradně **šifrovaným kanálem** (TLS 1.2 a vyšší).

Centrální správa logovacích politik

Konfigurace toho, **co a v jakém detailu** se na koncových stanicích sbírá, je řízena centrálně z webového rozhraní systému MS Custom LOG. Pro každou skupinu zdrojů (např. doménový řadič, souborový server, klientská stanice) lze samostatně definovat:

- výčet kanálů Windows Event Logu, které mají být sbírány (Security, System, Application, Setup, ForwardedEvents, případně vlastní kanály aplikací),

- výčet souborových a textových logů (např. IIS, DHCP debug, DNS debug, vlastní aplikační logy),

- úroveň podrobnosti (verbose / informational / warning / error),

- frekvenci a způsob přenosu (real-time stream vs. dávkové odesílání).

3.4 Vlastní konektory a vývoj vstupních zdrojů na míru

Systém MS Custom LOG podporuje širokou škálu předdefinovaných vstupních formátů, které pokrývají většinu běžně používaných technologií, protokolů a systémů v oblasti IT, bezpečnosti a provozu. Přesto může v některých případech nastat potřeba integrovat specifický systém, zařízení nebo formát dat, který není v základní nabídce podporovaných vstupů zahrnut.

Pro tyto účely nabízíme možnost vývoje vlastního konektoru na míru, který umožní připojení netypických nebo proprietárních zdrojů dat. Vývoj probíhá ve spolupráci s technickým týmem zákazníka a je plně přizpůsoben požadavkům na:

- datový formát a strukturu přenášených událostí,
- autentizační mechanismy a způsob připojení,
- požadovanou frekvenci nebo typ sběru (streaming, dávkově),
- způsob značkování a předzpracování dat.

Takto vytvořený modul se následně zařadí do běžného přehledu vstupních zdrojů v systému a je spravován stejným způsobem jako ostatní.

Pokud máte požadavky na vlastní konektor nebo integraci, která není v seznamu podporovaných vstupů, kontaktujte nás pro vyhodnocení a návrh řešení.

4 Parsery a zpracování dat

4.1 Použití předdefinovaných parserů

Předdefinované parsery představují základní způsob, jak systém MS Custom LOG transformuje a strukturuje vstupní logovací data. Parsery jsou implementovány prostřednictvím zpracovatelských pipeline, kde každá pipeline obsahuje sadu filtrů pro konkrétní typ vstupu (např. Syslog, Windows Event Log, Office365, CEF atd.).

Tyto parsery zajišťují:

- rozpoznání formátu zprávy,
- rozdělení textového logu na strukturovaná pole,
- normalizaci klíčových hodnot (čas, IP, uživatel, akce...),
- přiřazení značek (tagů) pro další zpracování nebo filtrování.

Jak parsery fungují v pozadí

Předdefinované parsery jsou založeny na kombinaci filtrů, zejména:

- grok – pro parsování textových vzorů,
- date – pro konverzi časových údajů do standardizovaného formátu,
- mutate – pro přejmenování polí, převod datových typů nebo odstranění nepotřebných polí,
- geoip – pro geografické informace na základě IP adresy,
- kv, json, csv – pro dekódování strukturovaných dat,
- add_field, add_tag – pro doplnění vlastních značek a metadat.

Každý parser je navržen tak, aby zvládl běžné varianty formátů konkrétního typu vstupu. Např. parser pro Syslog dokáže zpracovat zprávy dle RFC3164 i RFC5424 a extrahovat z nich hostname, facility, priority, message text, čas a další pole.

Aktivace parseru v systému

Při přidávání nového vstupního zdroje v sekci Management → Stack Management → Data sources, systém automaticky nabídne odpovídající parser podle zvoleného typu vstupu (např. Syslog → Syslog parser, Winlog → Windows parser atd.).

V případě potřeby lze u konkrétního vstupu ručně zvolit jiný parser nebo upravit nastavení existujícího (viz kapitola Tvorba vlastních parserů).

Výhody předdefinovaných parserů

- Okamžitě použitelné bez jakékoli konfigurace.
- Ověřené a stabilní – postavené na standardních šablonách a testovaných scénářích.
- Možnost kombinace s vlastními úpravami nebo doplňujícími filtry.
- Plná kompatibilita s ostatními funkcemi systému: tagování, dashboardy, alerty, exporty.

4.2 Tvorba vlastních parserů

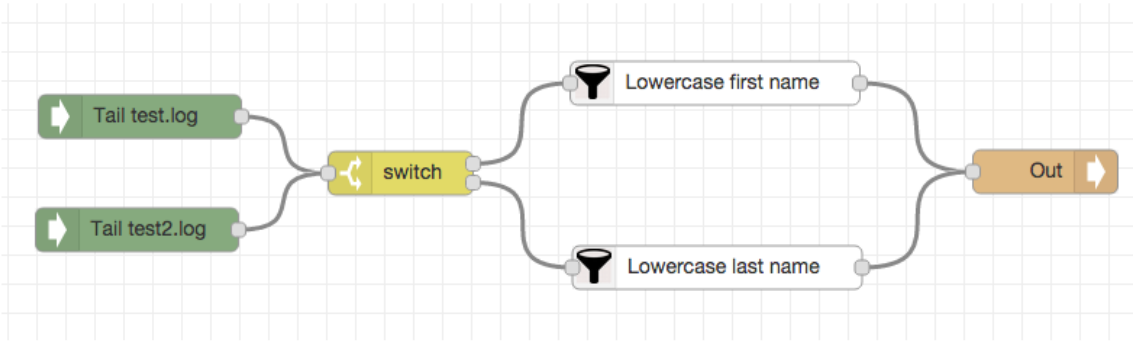
Systém MS Custom LOG umožňuje pokročilou tvorbu vlastních parserů prostřednictvím grafického rozhraní pro vizuální definici zpracovatelské logiky. Namísto psaní složitých textových konfigurací ve formátu Logstash pipeline umožňujeme administrátorům vytvářet parsery pomocí intuitivního grafického editoru, ve kterém jednotlivé kroky zpracování tvoří tzv. uzly (nody) propojené logickými vazbami.

Tento přístup výrazně zjednodušuje návrh, testování i údržbu parserů – není potřeba znát syntax Logstash konfigurací ani vytvářet složité regulární výrazy „naslepo“. Každý parser se skládá z vizuálního toku dat, kde je zřejmé, jak se log transformuje od vstupu až po výstup.

Přístup k editoru

V administrátorském rozhraní přejděte do nabídky:

- Management → Stack Management → Logstash pipelines.
- Klikněte na tlačítko „Nový parser“.
- Zvolte možnost „Grafické programování“ (namísto textového editoru).
- Otevře se vizuální editor s plátnem, na které lze vkládat uzly a propojovat je podle logiky zpracování.



Typy dostupných uzlů

Grafický editor obsahuje širokou knihovnu uzlů odpovídajících filtrům Logstash. Níže jsou popsány nejčastěji používané:

- Input node
  - Vstupní bod pro zpracování zprávy (např. textový řetězec ze Syslogu, JSON zpráva z Office365).
  - Lze jej připojit ke konkrétnímu zdroji nebo použít pro testovací data.
- Grok node
  - Slouží k parsování textového obsahu pomocí předdefinovaných šablon.
  - Umožňuje rozložit zprávu do strukturovaných polí (např. timestamp, user, action).
  - Obsahuje knihovnu běžně používaných vzorů, které lze snadno vybrat nebo upravit.
- Date node
  - Slouží k převodu časových údajů na jednotný formát (např. ISO 8601).
  - Umožňuje nastavit časové zóny, formát vstupu i výchozí hodnoty při chybě.
- Mutate node
  - Poskytuje operace nad poli: přejmenování, odstranění, přetypování (např. převod na integer nebo boolean), přidání nových polí.
  - Ideální pro standardizaci názvů nebo přípravu výstupu pro další vizualizace.
- Add tag / Remove tag
  - Umožňuje přidávat nebo odebírat značky (tagy) podle obsahu zprávy nebo výsledku filtrace.
  - Využívá se pro označení typu události (např. „neúspěšné přihlášení“, „chyba systému“).
- Condition (If/Then) node
  - Logická větev, která umožňuje větvení toku podle hodnoty pole nebo podmínky.
  - Vhodné pro tvorbu komplexních pravidel nebo různých cest zpracování v rámci jednoho parseru.

- GeoIP node
  - Načítá geografickou lokaci na základě IP adresy.
  - Výstupem je např. země, město, ISP nebo GPS souřadnice.
- JSON node
  - Rozebírá JSON zprávy na jednotlivá pole.
  - Umožňuje snadno zpracovávat API výstupy nebo události ve formátu RFC8259.
- Output node
  - Určuje, jak má být zpráva po zpracování odeslána dál.
  - Lze definovat výstupní index, typ dokumentu, případně dodat metadata.

Vytvoření parseru – příkladový scénář

Příklad: Vytváříme parser pro zprávy Syslog, které obsahují informaci o přihlášení uživatele.

1. Vložíme Input node, napojený na Syslog vstup.
2. Přidáme Grok node s šablonou pro rozložení zprávy na čas, IP a text události.
3. Použijeme If/Then node – ověříme, zda zpráva obsahuje „authentication failure“.
4. Větev „true“ spojíme s Add tag node – přidáme tag auth_fail.
5. Větev „false“ spojíme s Add tag node – přidáme tag auth_success.
6. Na závěr použijeme Output node s definicí výstupního indexu log-auth.

Parser tak dokáže v reálném čase rozlišovat úspěšná a neúspěšná přihlášení a zařazovat je podle značek.

Výhody grafického přístupu

- Přehlednost – jasná vizualizace zpracování krok za krokem.
- Bez programování – žádná potřeba psát složité regulární výrazy nebo textové konfigurace.
- Okamžité testování – možnost testovat parsery na reálných nebo testovacích datech přímo v editoru.
- Snadná správa a verzování – změny parserů lze sledovat, ukládat a případně vrátit.

V případě potřeby lze parsery dále kombinovat s vlastním tagováním a výstupními pravidly pro alerty, vizualizaci nebo notifikace. V další kapitole se budeme věnovat tagování a kategorizaci dat pro zjednodušené filtrování a vyhledávání.

4.3 Tagování událostí a klasifikace logů

Pro efektivní práci s rozsáhlými objemy logovacích dat je v systému MS Custom LOG klíčovým prvkem tagování událostí a jejich kategorizace. Pomocí tagů lze logy tematicky třídit, filtrovat, vizualizovat a využívat jako základ pro tvorbu alertů, přehledů i auditních výstupů.

Každá událost procházející zpracováním může být označena jedním nebo více tagy, které vystihují povahu nebo závažnost události, její původ, typ zařízení, stav apod.

Jak funguje tagování

Tagování je realizováno v parserech – konkrétně v rámci grafického editoru parserů. Vizuální uzly umožňují podle obsahu zprávy nebo struktury logu přidat konkrétní tagy. Ty jsou následně viditelné v grafickém rozhraní a slouží pro další práci s daty.

V pozadí se jedná o standardní mechanismus, kdy se pole tags přidává nebo upravuje v rámci průchodu zprávy filtrem.

Příklady běžně používaných tagů

- auth_success – Úspěšné přihlášení uživatele
- auth_fail - Neúspěšné přihlášení
- config_change - Změna konfigurace systému
- shutdown - Neočekávané vypnutí systému
- alert_critical - Událost vyžadující okamžitý zásah
- db_query - Událost související s databázovým dotazem
- network - Událost síťového typu

Uživatelé mohou definovat vlastní tagy dle provozních a bezpečnostních požadavků organizace.

Tvorba tagů pomocí grafického editoru

V editoru parserů lze tagování snadno realizovat pomocí uzlů:

- Condition (If/Then) node
  - Na základě hodnoty pole nebo obsahu zprávy větví logiku zpracování.
  - Např. „pokud zpráva obsahuje authentication failure, pokračuj touto větví“.
- Add tag node
  - Přidá specifický tag k události.
  - Může být napojen za podmínku nebo přímo na vstupní uzel.
- Remove tag node
  - Umožňuje odstranit automaticky přidaný tag, pokud je irelevantní (např. „_grokparsefailure“).
- Mutate node
  - Volitelně lze tagy transformovat nebo uložit jako jiná pole (např. event_type).
- Debug/Test node
  - Slouží pro testování, jaké tagy byly přidány – užitečné při ověřování parseru.

Práce s tagy ve výstupech

Po přidání tagů ve fázi zpracování parserem se tyto značky zobrazují v poli tags každého dokumentu v Elasticsearch.

V grafickém prostředí je pak možné:

- Filtrovat podle tagů v dashboardech, indexech i vyhledávání.
- Vytvářet vizualizace a statistiky na základě počtu výskytů konkrétních tagů.
- Definovat alerty (např. Watchery) na příchod události s daným tagem.
- Barevně odlišit závažné události (např. alert_critical) v přehledech.

Výhody přístupu

- Rychlá orientace v logech – není nutné analyzovat celý text zprávy.
- Podpora auditu a forenzní analýzy – lze filtrovat konkrétní typy událostí.
- Možnost vytváření pravidel a alertů bez programování.
- Standardizace napříč zdroji – různé formáty zpráv mohou sdílet společné tagy (např. „přihlášení“, „kritická chyba“).

4.4 Normalizace a enrichování dat

V systému MS Custom LOG je důležitou součástí zpracování logů tzv. normalizace (sjednocení struktury a významu dat) a enrichování (doplnění kontextu nebo hodnot). Tyto procesy zajišťují, že z různorodých logovacích zdrojů vznikne jednotný datový model, který lze snadno vyhledávat, vizualizovat a analyzovat bez ohledu na původní formát zprávy.

Tyto úpravy probíhají uvnitř parserů, které lze sestavovat ve vizuálním editoru pomocí přehledného grafického rozhraní.

Co znamená normalizace

Normalizace zahrnuje:

- Sjednocení názvů polí – např. src_ip, source_ip, client_ip → source.ip
- Převod datových typů – např. „200“ (string) → 200 (number)
- Standardizaci časových údajů – různé formáty časů na jednotný @timestamp
- Vyčištění nadbytečných nebo irelevantních dat
- Zachování konzistence napříč zdroji (i když mají různé struktury)

Například u přihlášení přes Windows, Syslog i VPN je cílem, aby výsledný dokument měl pole user.name, event.type a source.ip, bez ohledu na to, jak se tato data jmenovala v původní zprávě.

Co znamená enrichování (obohacování)

Enrichování slouží k doplnění dalších informací, které nejsou přímo obsaženy v přijaté zprávě, ale lze je dopočítat nebo vyhledat. Např.:

- GeoIP doplnění – podle IP adresy určujeme stát, město, ISP
- Kód → název – např. HTTP 404 → „Not Found“
- Doplnění organizační jednotky podle IP rozsahu
- Překlad UID uživatele na jméno
- Určení typu zařízení, aplikace, služby

Realizace ve vizuálním editoru parserů

Pomocí dostupných uzlů lze normalizaci a enrichování provádět bez psaní kódu:

- Mutate node
  - Převod názvů polí (rename)
  - Odstranění nepotřebných hodnot (remove_field)
  - Převedení typů (convert – např. na integer, boolean)
- GeoIP node
  - Na základě pole s IP adresou doplní údaje jako geo.country_name, geo.city_name, geo.location
- KV (key=value) node
  - Rozebere strukturovaný řetězec (např. user=admin status=fail) na jednotlivá pole
- Translate node
  - Nahrazuje hodnoty na základě mapy (např. 200 → OK, 404 → Not Found)
  - Lze využít pro výstupní obohacení nebo kategorizaci
- Add field node
  - Doplnění statického nebo vypočteného pole (např. log.source: firewall)
- If/Then node
  - Podmíněná enrichace – např. „pokud je port 22, nastav protocol: SSH“

Výstupní struktura po normalizaci

Po zpracování a enrichování by každý log měl obsahovat jednotná pole, jako např.:

```
{
  "@timestamp": "2025-07-09T10:20:15Z",
  "event.type": "authentication",
  "event.outcome": "failure",
  "user.name": "j.novak",
  "source.ip": "192.0.2.12",
  "geo.country_name": "Czech Republic",
  "log.source": "vpn"
}
```

Tato konzistentní struktura výrazně usnadňuje tvorbu dashboardů, vyhledávání i alertů.

Výhody normalizace a enrichování

- Lepší použitelnost dat – stejný dashboard funguje pro různé zdroje
- Vyšší přesnost analýz – díky typové správnosti a doplnění kontextu
- Snadná tvorba pravidel – jednotné podmínky pro alerty a vizualizace
- Možnost pokročilé korelace událostí

4.5 Filtrace a pravidla zpracování

Systém MS Custom LOG umožňuje definovat podmínky, za kterých mají být vstupní logy zpracovány, upraveny, obohaceny, nebo zcela vyřazeny. Filtrace slouží ke snížení objemu zpracovávaných událostí, zvýšení relevance dat a optimalizaci výkonu systému. Pravidla zpracování pak umožňují rozhodnout, jak s danou zprávou dále pracovat – například změnit pole, přidat značku, nebo přesměrovat zprávu do jiného indexu.

Všechny tyto mechanismy lze konfigurovat pomocí grafického programování ve vizuálním editoru parserů, bez nutnosti psát textové konfigurace nebo skripty.

Cíle filtrace

- Ignorovat nepotřebné nebo duplicitní zprávy
- Rozlišit závažné události od běžného provozu
- Směrovat různé typy zpráv do specifických výstupů
- Zajistit logickou větev zpracování pro různé typy zdrojů

Základní princip

Každá zpráva prochází vizuálně sestaveným tokem, ve kterém podmínkové uzly (If/Then) rozhodují, jak se s danou zprávou dále naloží. Na základě těchto podmínek lze:

- zprávu dále zpracovat (např. enrichovat),
- zprávu označit tagem (např. ignored),
- zprávu přesměrovat do jiného výstupu,
- zprávu zahodit (neindexovat vůbec),
- použít různé větve zpracování pro různé typy událostí.

Klíčové uzly pro filtrování

- If/Then node
  - Slouží jako rozcestník – na základě hodnoty pole rozhoduje o dalším směru zpracování.
  - Např. „pokud event.code = 200, pokračuj vpravo, jinak vlevo“.

- Drop node
  - Zprávu zcela zahodí – nebude indexována ani dále zpracována.
  - Vhodné pro zprávy typu „keep-alive“, „heartbeat“ apod.
- Add tag / Remove tag node
  - Označení zprávy pro budoucí výběr, filtrování nebo reporty.
- Mutate node
  - Možnost nastavit výchozí hodnoty polí pro zprávy, které nesplnily filtr.
- Output (conditional) node
  - Možnost odeslat zprávu do jiného indexu nebo složky podle typu obsahu.

Příklad scénáře

Cíl: filtrovat běžné události s event.severity: low a zpracovávat pouze varování a chyby.

- Použijeme If/Then node pro kontrolu pole event.severity.
- Větev low připojíme na Drop node.
- Větev medium a high pokračuje na obohacení (např. GeoIP, tagování).
- Výstupní node zapisuje do indexu logs-alerting.

Výsledkem je, že do indexu se dostanou pouze důležité zprávy a systém je nezatížen rutinním provozem.

Dynamická pravidla podle vstupu

Filtrace může být navázána i na zdroj logu, např.:

- jiná pravidla pro logy z firewallu než z webserveru,
- odlišné podmínky pro Windows vs. Linux,
- výjimky pro testovací zařízení (označené tagem test).

Vizuální editor umožňuje snadno kombinovat podmínky, negace i složitější logiku bez psaní kódu.

Výhody filtrování a pravidel

- Zmenšení objemu dat v úložišti
- Zvýšení relevance informací pro analytiky
- Optimalizace výkonu systému
- Jasná logika, snadno auditovatelná i upravitelná

5 Ukládání a integrita logovacích dat

Systém MS Custom LOG je navržen s důrazem na **dlouhodobou důvěryhodnost a forenzní použitelnost** uložených záznamů. Veškeré přijaté události jsou ukládány takovým způsobem, který zajišťuje jejich úplnost, časovou prokazatelnost a ochranu před neoprávněnou modifikací po celou dobu definované retenční doby. Architektura modulu vychází z principů ochrany auditních záznamů dle zákona č. 264/2025 Sb. o kybernetické bezpečnosti a navazujících mezinárodních standardů.

Tato kapitola popisuje, jakým způsobem systém zaručuje neměnnost dat, jejich jednoznačnou identifikaci, časovou prokazatelnost a odolnost vůči ztrátě v situacích zvýšené zátěže.

5.1 Důvěryhodné časové razítkování příchozích událostí

Každá příchozí událost je při příjmu opatřena dvěma na sobě nezávislými časovými údaji, které jsou ukládány v oddělených polích a v žádné následující fázi zpracování nejsou přepisovány:

- **Originální časová značka** (např. v poli `@original_timestamp`) -- převzatá beze změny ze zdrojového záznamu; slouží jako doklad o době vzniku události na straně zdroje,
- **Razítko příjmu systémem** (např. v poli `@ingest_timestamp`) -- generované systémem MS Custom LOG v okamžiku přijetí záznamu; slouží jako doklad o době, kdy se událost stala součástí auditovaného úložiště.

Razítko příjmu vychází z **interního zdroje přesného času** synchronizovaného protokolem NTP, případně PTP v prostředích s vyššími nároky na přesnost. Systém umožňuje volitelné napojení na externí **autoritu důvěryhodného času** v souladu se standardem RFC 3161 pro případy, kdy je vyžadováno kryptograficky podepsané razítko třetí stranou (např. pro vybrané kategorie auditních záznamů).

Detekce odchylky času

Systém průběžně vyhodnocuje rozdíl mezi originální značkou a okamžikem příjmu. Při překročení administrátorem nastavené mezní hodnoty je událost automaticky označena tagem (např. `time_skew_detected`) a může být spuštěno odpovídající upozornění. Tím je obsluze umožněno reagovat na výpadek synchronizace času nebo na případnou manipulaci s časem na straně zdroje.

5.2 Jednoznačná identifikace každého záznamu

Každému záznamu, který do systému vstoupí, je při příjmu přidělen **jednoznačný a neměnný identifikátor**. Identifikátor je tvořen kombinací dvou složek:

- **globálně jednoznačného ID** záznamu, přiděleného v okamžiku příjmu a zaručujícího nezaměnitelnost napříč všemi uzly systému,
- **kryptografického otisku původního obsahu zprávy** (např. v poli `raw_hash`), který umožňuje kdykoliv v budoucnu prokazatelně ověřit, že obsah záznamu nebyl po uložení změněn.

Konkrétní hashovací algoritmus je konfigurovatelný; ve výchozím nastavení je použit SHA-256, což umožňuje provozovateli reagovat na vývoj kryptografických doporučení bez zásahu do datového modelu. Identifikátor i otisk jsou nedílnou součástí každého uloženého dokumentu a jsou přenášeny do všech výstupních forem -- vyhledávacího rozhraní, exportů, reportů i REST API.

Touto kombinací je zajištěna nepřerušitelná **stopa záznamu (chain-of-custody)** od okamžiku jeho přijetí systémem až po případné předání orgánům činným v trestním řízení nebo NÚKIB pro účely forenzního vyšetřování.

5.3 Neměnnost uložených dat (režim WORM)

Auditní úložiště systému MS Custom LOG je provozováno v režimu **Write-Once-Read-Many (WORM)**. Po uložení záznamu do tohoto úložiště nelze obsah:

- mazat před uplynutím definované retenční doby,
- upravovat ani přepisovat,
- skrývat oprávněným uživatelům s rolí auditora.

Technické zajištění neměnnosti

Neměnnost je vynucována na úrovni datové vrstvy nezávisle na aplikační logice. Ani uživatelské účty s nejvyšším administrátorským oprávněním v běžném provozu nedisponují přístupovými právy, která by umožnila modifikaci surových auditních dat.

Retenční politika

Retenční doba je nastavitelná pro každý index, kategorii zdrojů nebo třídu citlivosti samostatně. Výchozí minimální hodnota odpovídá minimální době **18 měsíců**. Před uplynutím retence není možné záznamy odstranit, a to ani manuálním zásahem administrátora s nejvyššími oprávněními. Po uplynutí retence jsou data smazána řízeným způsobem a tato operace je rovněž zaznamenána do auditního deníku.

5.4 Ochrana integrity při zatížení a výpadku

Systém je navržen tak, aby ani při dočasné nedostupnosti úložiště nebo při krátkodobém přetížení nedošlo ke ztrátě, duplikaci nebo poškození záznamů. Toho je dosaženo kombinací několika nezávislých mechanismů:

- **Fronta na vstupu** - veškerá příchozí data jsou nejprve zapsána do fronty v paměti a teprve následně zpracována a indexována.

- **Spolehlivý transport s potvrzováním (back-pressure)** - pro zdroje podporující protokol RELP nebo syslog s potvrzováním systém využívá zpětnou vazbu, kterou informuje zdroj o nutnosti zpomalit přenos nebo zopakovat odeslání zprávy. Zdroj tedy nikdy nepovažuje zprávu za doručenou, dokud ji systém prokazatelně nepřevezme.

- **Kontrola dokončení zápisu** - žádný záznam není zdroji ani uživatelskému rozhraní označen jako přijatý dříve, než je trvale uložen, opatřen jednoznačným identifikátorem a kryptografickým otiskem.

Chování systému při dlouhodobém přetížení nad rámec kapacity fronty je konfigurovatelné. Administrátor může pro každou skupinu zdrojů zvolit mezi přístupem „**neztrácet, ale zpomalit**" (doporučeno pro auditní záznamy) a „**zahazovat nejstarší při přetečení**" (vhodné pro provozní telemetrii nižší důležitosti). Veškerá rozhodnutí o zahození jsou auditně zaznamenána.

5.5 Auditní deník přístupů ke kritickým operacím

Veškeré operace, které by mohly mít vliv na integritu, dostupnost nebo důvěrnost uložených záznamů, jsou samy zaznamenávány do odděleného **systémového auditního deníku**. Tento deník podléhá stejnému režimu neměnnosti (WORM) jako produkční auditní data a je oddělen od běžné administrace systému.

Sledovány jsou zejména následující kategorie operací:

- pokusy o smazání, úpravu nebo přejmenování indexů,
- změny retenčních politik a šifrovacích konfigurací,
- změny konfigurace zdroje času a synchronizace,
- změny rolí, oprávnění a přístupů k auditním datům,
- exporty většího rozsahu auditních dat mimo systém.

Auditní deník je dostupný v sekci Management → Audit → System Audit Log a je exportovatelný v podobě vhodné pro předání kontrolním a dozorovým orgánům.

5.6 Soulad s legislativou a normami

Mechanismy popsané v této kapitole zajišťují soulad systému MS Custom LOG s následujícími požadavky:

- **zákon č. 264/2025 Sb.**, o kybernetické bezpečnosti -- v ustanoveních upravujících uchovávání a ochranu auditních záznamů a poskytování součinnosti NÚKIB,

- **ISO/ČSN ISO/IEC 27001**, příloha A, kontroly A.8.15 (Logování) a A.8.16 (Monitorování činností),
- **RFC 3161** -- důvěryhodné časové razítkování (v případě využití externí TSA),
- standardní požadavky na **zachování důkazního řetězce (chain-of-custody)** pro účely forenzního vyšetřování.

Doporučení k provozu

- Při zavedení systému doporučujeme stanovit retenční dobu na nejméně 18 měsíců a režim WORM aktivovat již při prvním importu produkčních dat,
- Pro zdroje s nejvyšší důkazní hodnotou (autentizační systémy, privilegované účty, kritické aplikace) doporučujeme aktivovat napojení na externí autoritu důvěryhodného času (TSA),
- Minimálně 1× ročně doporučujeme provést kontrolní ověření integrity uložených záznamů namátkovým přepočtem kryptografických otisků na reprezentativním vzorku dat,
- Přístup k systémovému auditnímu deníku doporučujeme oddělit od běžných administrátorských rolí v souladu s principem rozdělení povinností (segregation of duties).

6 Dashboardy a vizualizace

6.1 Přehled prostředí dashboardů

Systém MS Custom LOG nabízí výkonné a flexibilní grafické uživatelské rozhraní pro tvorbu a správu dashboardů – interaktivních nástěnek, které zobrazují klíčové informace o stavu IT infrastruktury, bezpečnostních událostech, provozních incidentech a dalších logovaných datech v reálném čase.

Dashboardy slouží jako centrální pohled na provozní a bezpečnostní informace, které si každý uživatel může přizpůsobit svým potřebám. Mohou obsahovat různé vizualizační komponenty, jako jsou grafy, tabulky, mapy, měřidla či seznamy událostí, a to s možností filtrování, dynamického přepínání období a okamžitého drill-downu do detailů.

Navigace a uživatelské prostředí

Přístup k dashboardům je dostupný přes hlavní menu pod sekcí „Nástěnky / Dashboardy“. Po otevření rozhraní uživatel vidí:

- Seznam existujících dashboardů (název, popis, datum poslední úpravy),
- Možnost vytvoření nového dashboardu,
- Možnost hledání, kopírování, exportu nebo odstranění dashboardu.
- Dashboardy lze filtrovat podle přístupových práv, značek nebo uživatelské role.

Komponenty dashboardu

Každý dashboard je tvořen jednotlivými panely (komponentami), které zobrazují konkrétní datové výstupy. Mezi nejběžnější typy komponent patří:

- Časové řádkové grafy – vývoj událostí v čase,
- Sloupcové grafy – porovnání kategorií (např. typ událostí, systémy),
- Datové tabulky – seznam událostí seřazený podle času nebo důležitosti,
- Tachometry a měřidla – aktuální hodnoty (např. počet kritických incidentů),
- Mapa světa – geografické zobrazení událostí podle IP (GeoIP),
- Koláčové grafy – rozložení podle typů zařízení, aplikací, uživatelů apod.

Každý panel může být interaktivní – kliknutím lze otevřít podrobnosti nebo aplikovat filtr na celý dashboard.

Práce s daty a filtry

Dashboardy podporují interaktivní filtrování:

- podle časového rozsahu (např. posledních 15 minut, 24 hodin, vlastní období),
- podle hodnot v jednotlivých polích (uživatel, IP adresa, zdroj…),
- pomocí předdefinovaných značek nebo typů událostí (např. auth_fail, error, firewall).

Filtry lze kombinovat a dynamicky měnit bez potřeby přepínání dashboardu.

Možnosti zobrazení

Uživatelé mají plnou kontrolu nad vzhledem dashboardu:

- přetahování komponent myší,
- změna velikosti, barvy, typu vizualizace,
- seskupení panelů do sekcí (např. „Bezpečnost“, „Provoz“, „Síť“),
- uložení vlastních verzí nebo šablon.

Každý dashboard lze exportovat do formátu PDF, PNG nebo JSON pro sdílení nebo archivaci.

Přístup a oprávnění

Každý dashboard může být:

- privátní (dostupný jen danému uživateli),
- sdílený v rámci role (např. analytici, bezpečnostní tým),
- veřejný – zobrazitelný bez přihlášení (např. na velkoplošné obrazovce v dohledovém centru).

Oprávnění k úpravě a zobrazení se spravují prostřednictvím systému rolí.

Dashboardy tvoří základní pracovní prostředí pro sledování aktuálního stavu systému, bezpečnostních událostí i historických trendů. V následující kapitole se zaměříme na tvorbu a úpravu dashboardů – od přidání prvního panelu až po definici vlastních vizualizací.

6.2 Tvorba, editace a publikace dashboardů

Systém **MS Custom LOG** umožňuje oprávněným uživatelům jednoduše vytvářet vlastní dashboardy, upravovat stávající přehledy a publikovat je pro další členy týmu. Tvorba dashboardů probíhá přímo v uživatelském rozhraní pomocí vizuálního nástroje typu drag-and-drop, bez nutnosti psát kód nebo SQL dotazy.

Vytvoření nového dashboardu

- Vstup do sekce dashboardů
  - V hlavním menu zvolte sekci „Nástěnky / Dashboardy“ a klikněte na tlačítko „Vytvořit nový dashboard“.
- Zadání základních údajů
  - Název dashboardu – např. „Síťový provoz – firewall“.
  - Volitelný popis – určení účelu, zaměření, typ dat.
- Otevře se prázdná pracovní plocha, připravená pro přidávání panelů (vizualizací).

Přidání vizualizačního panelu

- Klikněte na tlačítko „Přidat panel“ a zvolte typ vizualizace:
  - Časová osa (line chart),
  - Sloupcový graf (bar chart),
  - Datová tabulka (data table),
  - Měřidlo (gauge),
  - Mapa (regiony podle IP),
  - Koláčový graf,
  - A další…
- Vyberte datový index, ze kterého má vizualizace čerpat data (např. logs-*).
- Definujte podmínky pro zobrazení:
  - pole (např. event.type, source.ip, user.name),
  - agregační funkce (počty, průměry, součty),
  - časový rozsah (např. posledních 24 hodin).
- Panel lze přetahovat, měnit velikost, barvy a umístění na dashboardu.

Úpravy a správa dashboardu

- Úprava existující vizualizace

    - Kliknutím na ikonu tužky otevřete konfiguraci a upravíte dotazy, typ zobrazení nebo vzhled.
- Duplikace a přesun panelů
    - Vizualizace lze jednoduše kopírovat a přeuspořádávat pomocí myši.
- Přidání filtrů a ovládacích prvků
    - Dashboardy mohou obsahovat globální filtry, časové rozsahy, přepínače a dropdowny, které ovlivňují všechny panely najednou.

Uložení a publikace dashboardu

Po dokončení návrhu lze dashboard:

- Uložit jako koncept (pouze pro autora),
- Publikovat pro zvolenou uživatelskou roli (např. síťový tým, dohledové centrum),
- Nastavit jako výchozí dashboard pro konkrétní roli nebo uživatele,
- Exportovat jako šablonu (např. do JSON formátu pro přenos mezi prostředími),
- Zamknout před úpravami, aby zůstal jednotný napříč uživateli.

Praktické tipy

- Používejte standardizované názvy panelů pro snadnou orientaci.
- Testujte dashboardy na historických datech, než je zpřístupníte širšímu publiku.
- Kombinujte různé typy vizualizací – grafy, tabulky, mapy pro lepší přehled.

Tvorba dashboardů v MS Custom LOG je navržena s důrazem na jednoduchost, rychlost a intuitivní ovládání. Uživatelé se tak mohou soustředit na analýzu dat, nikoliv na technické aspekty zobrazování.

6.3 Vizualizační komponenty a datové zdroje

V systému MS Custom LOG jsou vizualizace klíčovým nástrojem pro přehlednou prezentaci a analýzu logovaných událostí. Pomocí intuitivního grafického rozhraní lze vytvářet vizualizační komponenty, které čerpají z libovolných datových zdrojů indexovaných v systému. Tyto komponenty je možné dále kombinovat v rámci dashboardů, sdílet a exportovat.

Typy vizualizačních komponent

Uživatel má na výběr z několika základních vizualizačních formátů, které lze podle potřeby kombinovat a parametrizovat:

- Časová osa (Line chart)
    - Zobrazuje vývoj určité hodnoty v čase, např. počet událostí za poslední hodiny, dny, týdny.
- Sloupcový graf (Bar chart)

    - Vhodný pro porovnání četností různých kategorií, např. typy zařízení nebo událostí.
- Koláčový graf (Pie chart)
    - Zobrazení rozložení mezi jednotlivé hodnoty (např. podíl typů protokolů).
- Datová tabulka (Data table)
    - Umožňuje podrobné zobrazení událostí ve formě řádků se všemi relevantními poli.
- Měřidlo (Gauge / Goal)
    - Zobrazuje aktuální hodnotu vůči cílové hodnotě nebo maximu (např. počet varování za den).
- Mapa (Region map / Coordinate map)
    - Vizualizace geografických informací (např. IP adresy) s využitím GeoIP obohacení.
- Heatmapa
    - Intenzita výskytu událostí v čase a kategoriích – například přetížení systému během konkrétních hodin.
- Tag cloud (Mrak slov)
    - Zobrazení nejčastějších hodnot daného pole, např. nejčastější názvy služeb nebo uživatelů.

Datové zdroje vizualizací

Každá vizualizace je založena na tzv. datovém pohledu (index pattern), který definuje, jaká data budou do grafu načítána. Typicky se jedná o:

- Indexy dle typu zařízení nebo systému (např. logs-firewall-*, logs-windows-*),
- Indexy dle prostředí (např. logs-production, logs-test),
- Kombinace více zdrojů přes zástupné znaky (např. logs-*).

Při vytváření vizualizace uživatel vybere:

- Datový zdroj – index nebo pattern dat, který bude použit.
- Agregační funkce – např. počet výskytů, suma, průměr, maximální hodnota.
- Pole pro zobrazení – např. event.type, source.ip, host.name, user.name.
- Časové pole – např. @timestamp, podle kterého se data řadí.

Vizualizace dále podporují přepínání časového rozsahu a použití interaktivních filtrů.

Možnosti konfigurace

U každé vizualizace lze nastavit:

- Název a popis komponenty,
- Styl zobrazení – barvy, osy, legendy, velikost prvků,
- Filtrování – globální nebo specifické pro daný panel,
- Třídění dat – např. podle četnosti, abecedně, nebo podle vlastního pořadí,
- Omezení počtu zobrazených hodnot (např. top 10 protokolů).

Příklady použití

- Bezpečnostní přehled: sloupcový graf podle event.severity, tabulka kritických událostí, GeoIP mapa.
- Síťový monitoring: časová osa přenosů, rozdělení zdrojových IP, tag cloud názvů aplikací.
- Auditní logy: tabulka přihlášení, výskyt událostí podle uživatelů, měřidlo počtu chybových kódů.

Vizualizační komponenty tvoří základ pro efektivní práci s daty. Jejich správnou kombinací lze rychle odhalit anomálie, sledovat vývoj událostí a získat strategický přehled o celém systému.

6.4 Interaktivní filtrování a drill-down do detailů

Pro efektivní práci s vizualizacemi a dashboardy poskytuje systém MS Custom LOG rozsáhlé možnosti interaktivního filtrování a procházení detailních informací. Díky těmto funkcím mohou uživatelé rychle vyhledávat konkrétní události, analyzovat souvislosti a identifikovat příčiny problémů bez nutnosti opouštět grafické rozhraní.

Interaktivní filtrování

Každý dashboard obsahuje horní panel s globálními filtry, které ovlivňují všechny vizualizace zároveň. Uživatelé mohou:

- Zvolit časové období – výběr z přednastavených rozsahů (např. „posledních 15 minut“, „včera“, „posledních 7 dnů“) nebo definovat vlastní interval s přesností na sekundy.
- Přidat filtry podle polí – např. source.ip = 10.0.0.1, event.type = login_failure, user.name contains admin.
- Použít logické operátory – a zároveň, nebo, není, neobsahuje.

Využít klikací filtry přímo z vizualizací – kliknutím na prvek grafu (např. bar, segment koláče, řádek tabulky) se automaticky přidá odpovídající filtr.

Aktivní filtry jsou vždy viditelné a mohou být jednoduše odstraněny nebo upraveny.

Drill-down do detailních dat

Při práci s agregovanými přehledy může uživatel kdykoli přejít na detailní zobrazení konkrétních událostí (tzv. drill-down), a to několika způsoby:

- Kliknutí na vizualizační prvek – např. sloupec, hodnota v tabulce, bod v grafu.
- Volba akce „Zobrazit podrobnosti“ – dostupná u většiny komponent.

- Přesměrování do detailního přehledu událostí – otevře se záznamová tabulka s přesnými hodnotami všech polí daných záznamů (např. čas, zdroj IP, cíl, typ události, hlavičky, zpráva apod.).

Zobrazení syrových logů

Kromě agregovaných dat lze zobrazit i surové zprávy v tzv. datové prohlížečce:

- Seznam událostí v chronologickém pořadí,
- Možnost řazení podle času, závažnosti, typu,
- Vyhledávání pomocí klíčových slov, regulárních výrazů nebo přesných hodnot,
- Zobrazení všech dostupných polí včetně metadat (značky, původní zpráva, parsované části).

Uživatel tak může plynule přejít od souhrnného přehledu k jednotlivým událostem, a zpětně si zafiltrovat dashboardy dle zjištěných hodnot.

Interaktivní filtrování a drill-down představují zásadní nástroj pro každodenní práci analytiků, operátorů i auditorů. Díky nim je možné rychle reagovat na incidenty, ověřit hypotézy nebo prohloubit analýzu bez nutnosti přepínání mezi nástroji.

7 Reporty a notifikace

7.1 Tvorba a plánování reportů

Systém MS Custom LOG umožňuje automatizované generování přehledů (reportů) z vybraných dashboardů a jejich pravidelné doručování oprávněným uživatelům. Tato funkcionalita slouží jak pro provozní monitoring, tak pro auditní účely, bezpečnostní dohled nebo management.

Možnosti výstupu

Reporty lze generovat v následujících formátech:

- PDF – vhodné pro prezentaci, tisk nebo archivaci,
- PNG / obrázek dashboardu – pro vizuální přehled ve zjednodušené formě,
- CSV – export datových tabulek do tabulkového procesoru (např. Excel),
- JSON – pro automatizované zpracování jinými systémy.

Tvorba nového reportu

- Přejděte do sekce Správa → Reporty.
- Klikněte na „Vytvořit nový report“.
- Vyplňte základní údaje:
  - Název reportu (např. „Síťové události – denní report“),

- Zdroj dat: výběr existujícího dashboardu, ze kterého se report vygeneruje,
- Formát výstupu: PDF, PNG, CSV, atd.
- Rozsah dat: např. posledních 24 hodin, posledních 7 dnů, vlastní časový interval.

Plánování automatického odesílání

Po vytvoření reportu lze nastavit pravidelné zasílání:

- Frekvence odesílání:
  - Denně (např. každý den v 7:00),
  - Týdně (např. každé pondělí),
  - Měsíčně (např. první den v měsíci),
  - Vlastní cron výraz pro pokročilé nastavení.
- Způsob doručení:
  - E-mailem – zadání adresátů (včetně více uživatelů),
  - Uložení do složky – například na připojené úložiště nebo FTP,
  - Webhook / API volání – odeslání do externího systému pro další zpracování.
- Podmínky pro odeslání (volitelně):
  - Odeslat pouze při splnění podmínky (např. výskyt události s kritickou závažností),
  - Odeslat jen pokud došlo ke změnám od posledního reportu.

Správa existujících reportů

V přehledu reportů lze:

- Upravovat nastavení (včetně frekvence a adresátů),
- Aktivovat/deaktivovat plánování bez mazání konfigurace,
- Manuálně spustit vygenerování a doručení (např. pro okamžitý export),
- Prohlížet historii generovaných výstupů a jejich stav.

Příklad využití
Administrátor nastaví automatické zasílání PDF reportu „Přehled kritických bezpečnostních událostí“ každý den v 6:00 na e-maily bezpečnostního týmu. Report obsahuje dashboard se statistikami, časovou osou a detailní tabulkou posledních incidentů.

7.2 Definice upozornění (alertů)

Systém MS Custom LOG umožňuje definovat automatické upozornění (alerty) na základě detekovaných událostí nebo podmínek v datech. Alerty slouží k včasnému varování operátorů, bezpečnostních týmů nebo administrátorů při výskytu neočekávaných nebo rizikových situací. Výhodou je možnost okamžité reakce bez nutnosti trvalého dohledu nad dashboardy.

Vytvoření nového alertu

- Přejděte do sekce Správa → Upozornění / Alerty.
- Klikněte na tlačítko „Vytvořit nový alert“.
- Vyberte typ alertu dle způsobu vyhodnocení:
  - Na základě datového dotazu – definice konkrétního filtru nad indexem (např. event.severity = critical AND host.name = firewall-01).
  - Na základě metrik – počet výskytů událostí za časové období (např. více než 10 chybových přihlášení za 5 minut).
  - Na základě agregací z dashboardu – např. když se počet událostí překročí určitou mez v existující vizualizaci.
  - Porovnání s historickými daty – např. náhlý nárůst oproti obvyklému stavu.

Konfigurace alertu

Při tvorbě alertu je možné nastavit:

- Název – výstižný název pro přehlednost a vyhledávání (např. „Brute-force na SSH“),
- Podmínka spuštění – např. „Počet je větší než“, „Hodnota obsahuje text“, „Výskyt pole není nulový“,
- Časový rozsah vyhodnocení – za posledních X minut,
- Frekvence vyhodnocování – např. každou minutu, každých 5 minut, dle potřeby,
- Zpoždění / vyrovnání špiček – volitelné zdržení reakce, pokud je potřeba eliminovat falešné poplachy.

Akce alertu

Po splnění podmínky lze automaticky spustit jednu nebo více akcí:

- Odeslání e-mailu – s vlastní předlohou a proměnnými (např. hostname, počet výskytů),
- Syslog notifikace – pro přeposlání do jiného systému nebo SIEM nástroje,
- Webhook (HTTP volání) – např. zaslání na interní systém nebo integrační službu,
- Záznam do logu – interní logování výskytu alertu pro auditní účely.

Každá akce může mít definován vlastní kanál, příjemce a obsah zprávy.

Správa a historie alertů

V rozhraní pro správu alertů je dostupné:

- Seznam aktivních a neaktivních alertů, jejich stav a čas posledního spuštění,
- Záznam historie – kdy a kolikrát byl alert spuštěn a jaká akce byla provedena,
- Možnost pozastavení alertu bez jeho smazání,
- Duplikace alertu pro snadné vytvoření podobné podmínky.

Příklad využití

Uživatel vytvoří alert, který každých 5 minut vyhodnocuje výskyt chybových přihlášení (event.type = login_failed). Pokud je zaznamenáno více než 20 případů z jedné IP adresy v daném období, systém automaticky zašle upozornění e-mailem administrátorovi a zároveň odešle Syslog zprávu do NOC centra.

Díky systému alertů lze výrazně snížit čas potřebný k reakci na bezpečnostní i provozní incidenty. Nastavením správných podmínek se systém stává nejen nástrojem pro analýzu, ale i pro aktivní dohled a ochranu prostředí.

8 Rozhraní API a integrace

8.1 REST API

Systém MS Custom LOG poskytuje otevřené a dokumentované REST API rozhraní pro přístup k uloženým logovacím datům, metadatům a analytickým dotazům. Toto rozhraní je určeno především pro čtení dat, práci s indexy a analytické operace. Umožňuje také pokročilé vyhledávání, agregace a export informací pro další využití v externích systémech.

API je navrženo jako RESTful služba, využívající standardní HTTP metody (GET, POST, PUT, DELETE) a přenášející data ve formátu JSON.

Klíčové vlastnosti REST API

Prostřednictvím REST API lze:

- Dotazovat se na logy pomocí strukturovaných nebo fulltextových požadavků,
- Filtrování a agregace dat dle časového rozsahu, závažnosti, typu události, zařízení apod.,
- Získávat trendy, statistiky a přehledy, např. histogram výskytů, top zdroje, atd.,
- Exportovat data včetně výsledků dotazů do externích systémů,
- Spravovat indexy a metadata, např. schéma, mappings nebo aliasy.

Dokumentace a specifikace

Systém využívá osvědčené a veřejně dokumentované rozhraní pomocí specifikace OpenAPI. Kompletní specifikace REST API je dostupná online ve formě technické dokumentace, kde jsou podrobně popsány všechny podporované operace:

https://www.elastic.co/docs/api/doc/elasticsearch/

Příklad integrace se systémem Zabbix

Scénář: Získání poslední kritické události z logů

Zabbix může pomocí externího skriptu nebo webhooku (HTTP agent item) pravidelně volat REST API systému a dotazovat se například:

POST https://log.ms-custom.local/logs-critical/_search

Tělo požadavku:

```
{
  "size": 1,
  "query": {
    "bool": {
      "must": [
        { "match": { "severity": "critical" } },
        { "range": { "@timestamp": { "gte": "now-5m" } } }
      ]
    }
  },
  "sort": [{ "@timestamp": { "order": "desc" } }]
}
```

Odpověd může vypadat:

```
{
  "hits": {
    "total": { "value": 1 },
    "hits": [
      {
        "_source": {
          "message": "Firewall dropped connection from 10.0.0.12",
          "@timestamp": "2025-07-08T12:34:56Z",
          "host": "fw01",
          "severity": "critical"
        }
      }
    ]
  }
}
```

Nastavení v Zabbixu

V Zabbixu je třeba:

- Vytvořit novou šablonu nebo hosta, ke kterému chcete logy přiřadit.
- Přidat nový item typu HTTP agent:
  - Typ: HTTP agent

  - Metoda: POST
  - URL: https://log.ms-custom.local/logs-critical/_search
  - Tělo požadavku: (viz výše)
  - Hlavička: Authorization: Bearer <token>, Content-Type: application/json
  - Interval: např. každých 60 sekund
- Definovat trigger, který upozorní na nalezený výskyt (např. pokud odpověď obsahuje hits.total.value > 0).

9 Správa systému

9.1 Zálohování a obnova dat a konfigurace

Spolehlivé zálohování a možnost obnovy dat a konfiguračních nastavení je klíčovou součástí provozu systému MS Custom LOG. Tento systém poskytuje nástroje pro pravidelné zálohování dat, konfigurací i vizualizačních prvků, a zároveň umožňuje jejich selektivní nebo úplnou obnovu v případě potřeby – například při havárii, migraci nebo testování.

Typy zálohovaných dat

Systém podporuje zálohování následujících oblastí:

- Indexovaná logovací data (logy, události, obohacené záznamy),
- Konfigurace vstupních zdrojů a jejich parametry,
- Parsery a logické toky zpracování dat,
- Uživatelské role a oprávnění,
- Dashboardy, vizualizace a reporty,
- Definice alertů, pravidel a notifikací.

Možnosti zálohování

Zálohování lze provádět:

- Plně automatizovaně (doporučeno)
  - Pomocí plánovaného úkolu (např. denně v 2:00),
  - Exportuje se celý stav systému nebo zvolené části (data, konfigurace, nebo obojí),
  - Zálohy jsou ukládány do specifikované složky nebo vzdáleného úložiště (např. NAS, FTP, cloud).
- Manuálně přes správní rozhraní
  - Přes rozhraní Management → System → Backup lze:
  - vytvořit jednorázovou zálohu,
  - zvolit typ dat (konfigurace / logy / vše),
  - stáhnout zálohu jako soubor pro offline uložení.

Obnova dat a konfigurace

Obnovu lze provést:

- V sekci Management → System → Restore lze:
- nahrát záložní balíček nebo jej zvolit z vzdáleného úložiště,
- zvolit rozsah obnovy (např. pouze konfigurace bez dat),
- systém upozorní na přepsání existujících dat.

Doporučení k zálohování

- Provádějte denní automatické zálohy konfigurace (parsery, dashboardy, pravidla),
- Zálohujte data dle objemu logů a retenční politiky (např. 1× denně u kritických systémů, 1× týdně u zbylých),
- Zálohy ukládejte mimo produkční prostředí – ideálně do odděleného bezpečného úložiště,
- Testujte obnovu pravidelně na neprodukčním prostředí (ověření integrity),
- Zabezpečte přístup k zálohám šifrováním a řízením přístupových práv.

9.2 Sledování stavu systému a telemetrie

Správné fungování systému **MS Custom LOG** závisí nejen na samotném sběru a analýze logů, ale i na **kontinuálním dohledu nad stavem infrastruktury** a jednotlivých komponent systému. Pro tento účel je k dispozici vestavěný modul pro **sledování výkonu, dostupnosti a diagnostiky**, který poskytuje přehledy o zdraví jednotlivých částí systému, jejich zatížení a provozních metrikách.

Sledované komponenty

Monitoring zahrnuje následující části:

- Indexační službu (vyhledávací engine, repliky, stav shardů),
- Datové toky a zpracování logů (pipeline, fronty, latence),
- Stav úložiště a datových uzlů (disková kapacita, IO),
- Zátěž jednotlivých instancí (RAM, CPU, thread pool),
- Zdraví clusteru jako celku (stav: zelený, žlutý, červený).

Zobrazené metriky

Monitorovací rozhraní zobrazuje například:

- Zdraví clusteru (včetně důvodů degradace),
- Počet indexovaných dokumentů za minutu,
- Délku front pro zpracování dat (Logstash pipeline),
- Vytížení heap paměti, garbage collection,
- Počet otevřených indexů, segmentů a shardů,
- Disková kapacita jednotlivých uzlů a její využití,
- Upozornění na stav uzlů (offline, zpomalení, varování).

Telemetrie

Systém také využívá interní telemetrické sběry dat, které slouží ke:

- Statistickému vyhodnocení používání systému (počet dashboardů, aktivních uživatelů apod.),
- Optimalizaci výkonu – identifikace pomalých dotazů, příliš velkých indexů atd.,
- Zjišťování potenciálních problémů před jejich vznikem (např. překročení mezí heap paměti).

Upozornění a reakce

V případě, že dojde k:

- Zhoršení dostupnosti uzlu,
- Překročení definovaného limitu kapacity,
- Příliš vysokému zatížení některé části systému,

je možné aktivovat automatické upozornění pomocí přednastavených alertů (viz kapitola 7.2), např. e-mail, syslog nebo webhook.

Historie výkonu a zpětné sledování

Všechny metriky jsou ukládány časově a lze:

- Zobrazit vývoj v čase (např. za posledních 7 dní),
- Exportovat časové řady pro další analýzu,
- Porovnávat provozní stavy mezi různými časovými úseky (např. před a po aktualizaci systému).

Doporučení

- Aktivně sledujte stav clusteru minimálně 1× denně,
- Nastavte notifikace pro události, které mohou mít dopad na provoz (např. degradace výkonu, nedostatek místa),
- Pravidelně vyhodnocujte vývoj systémového zatížení a plánujte případné škálování.

9.3 Upgrade a Downgrade systému

Systém MS Custom LOG podporuje řízený proces aktualizací (upgrade) i řízený návrat na předchozí verzi (downgrade). Tyto operace lze provádět jak v plně připojeném online režimu, tak i v prostředí bez přístupu k internetu – tedy v offline režimu.

Typy verzí

Verzování systému je řízeno pomocí standardního schématu:

MAJOR.MINOR.PATCH
např. 2.7.4

- Patch verze – opravné balíčky (bez zásahu do struktury dat),
- Minor verze – přidávají nové funkce,
- Major verze – mohou měnit strukturu dat nebo konfiguraci, vyžadují speciální pozornost.

Postup aktualizace

Před každou aktualizací se důrazně doporučuje provést:

- Kompletní zálohu dat a konfigurace (viz kap. 9.1),
- Kontrolu kompatibility všech komponent (vstupní zdroje, dashboardy, parsery),
- Vyhodnocení stavu systému – dostupnost uzlů, dostatek volné kapacity.

Online aktualizace
- Probíhá automaticky přes administrátorské rozhraní nebo skriptované příkazy,
- Systém se připojí k repozitáři a stáhne ověřené balíčky,
- Aktualizace je řízena systémem, uživatel pouze potvrzuje kroky.

Offline aktualizace
- Určeno pro prostředí bez přístupu k internetu (např. uzavřené sítě),
- Správce stáhne instalační balíčky ze zákaznického portálu a nahraje je do systému ručně,
- Spuštění aktualizace probíhá přes administrační rozhraní

Pořadí a pravidla verzí

Před aktualizací na vyšší major verzi (např. z 2.x na 3.0) je nutné nejprve systém aktualizovat na nejvyšší dostupnou minor verzi stávající řady (např. 2.9.x),

Tento postup zajišťuje postupnou migraci a kontrolu kompatibility.

Příklad:
Při přechodu z verze 2.5.3 na 3.0.0 je třeba nejprve provést upgrade na 2.9.x.

Downgrade systému
- Downgrade je možný pouze o jednu verzi níže (např. z 3.0 na 2.9),
- Provádí se pouze v případech kritických problémů (např. nekompatibilita po upgrade),
- Systém před downgrade automaticky ověřuje dostupnost předchozích záloh,
- Downgrade není možný bez existující zálohy dat a konfigurace pro danou verzi.

Doporučení

- Neprovádějte aktualizace bez záloh a kontroly systémových prostředků,
- Testujte nové verze nejprve na neprodukčním prostředí,
- Dodržujte doporučené pořadí verzí a pravidla přechodu mezi řadami,
- Využívejte výpis změn (changelog) k seznámení s novinkami a úpravami v každé verzi.