



» LOGmanager Best Practice návod - Integrace s Flowmon

Flowmon monitoruje síťový provoz a dokáže vyhodnotit, zda v něm nedochází k anomáliím či útokům. Také dokáže sledovat, jak fungují používané aplikace (včetně cloudových), jak se chovají uživatelé v síti, servery a jejich služby apod. či zda se jejich chování nějakým způsobem změnilo - a upozorní administrátora. Pro útočníka znamená nasazení Flowmonu v síti velkou překážku, jelikož je z pohledu provozu v síti neviditelný, a útočník jej tak nedokáže odhalit a ovlivnit záznamy.

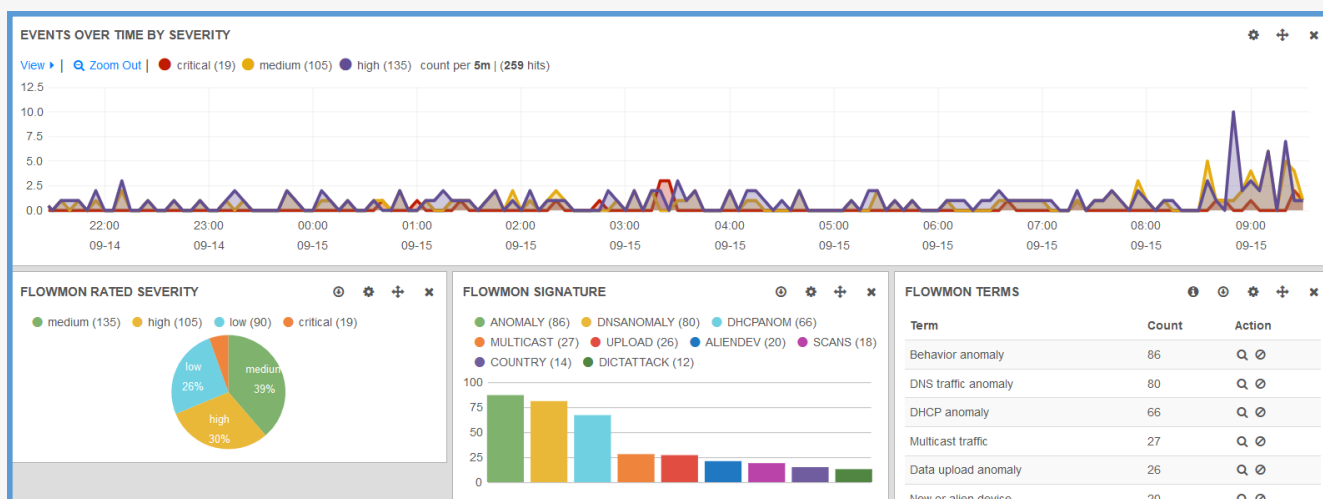
LOGmanager se naopak soustředí na informace, které získává z jednotlivých zařízení komunikujících v síti. Dokáže tak upozornit na nestandardní chování uživatelů (včetně pokusu o zcizení dat) a dává možnost identifikovat i provozní stavy koncových zařízení. Zjednodušeně lze říci, že pošle-li zařízení či jakýkoliv zdroj v síti informaci o události, LOGmanager ji detailně zpracuje, dlouhodobě uloží, umožní její snadnou interpretaci, provázání s daty jiných systému a zamezí jakékoliv možné manipulaci s jejím obsahem.

Z tohoto stručného popisu je zřejmé, že obě řešení mají v organizaci své místo a proto dává smysl je vzájemně integrovat.

» Možnosti integrace

Níže jsou v bodech stávající možnosti integrace:

- Sběr, dlouhodobé uchování a viditelnost do logů Flowmon v LOGmanageru** - Defaultní integrace, kde dle návodu v dokumentaci LOGmanager lze snadno nastavit odesílání logů z Flowmon do LOGmanageru. Díky vestavěné klasifikaci není třeba žádných konfiguračních změn na straně LOGmanageru k důkladnému zpracování a detailní vizualizaci Flowmon dat v perspektivě ostatních síťových a bezpečnostních řešení organizace.
- Obohacení logů Flowmon zpracovaných na straně LOGmanageru o dodatečná metadata** - součástí LOGmanager vestavěných upozornění je i vzorové upozornění nazvané „Flowmon_log_enhancement“. Tento „alert“ po aktivaci provádí doplnění metadat v LOGmanageru o URL link směřující na detail události do Flowmon GUI. Proklikem v rozhraní LOGmanageru je tak uživatel přímo přesměrován do konzole Flowmon s popisem daného incidentu.
- Doplnění uživatelské identity z Microsoft AD do prostředí Flowmon** - Flowmon umožňuje prostřednictvím vlastního syslog kolektoru přijímat data pro obohacení událostí o identitu uživatelů. Přesněji řečeno - kým byla ve chvíli vzniku události dle MS AD používána daná IP adresa). LOGmanager tyto informace již získává v rámci sběru všech auditní politikou AD definovaných logů vlastním Agentem (LOGmanager WES). Tyto logy zpracovává a na základě jednoduchého alertu umožní logy ve strukturovaném formátu předat do Flowmon, který je použije pro další obohacení vlastních dat.



Obrázek: náhled vizualizace Flowmon dat v LOGmanageru

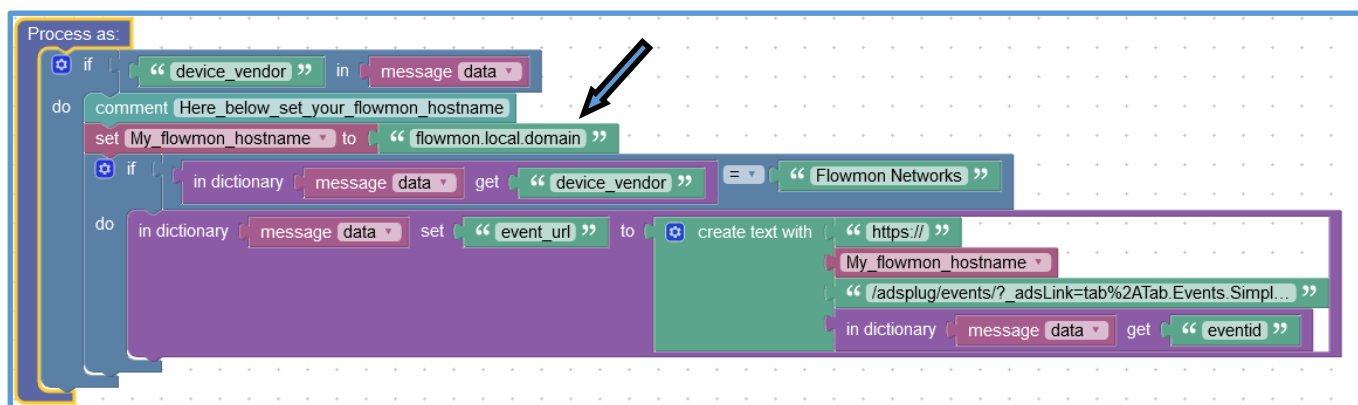
» 1. Sběr, dlouhodobé uchování a viditelnost do logů Flowmon:

Zde je integrace velmi snadná, pro dosažení základní integrace postupujte dle online dokumentace LOGmanageru v menu: *LOGmanager dokumentace / Zdrojová zařízení a aplikace / Flowmon*. Celý postup se sestává jen z šesti snadných kroků.

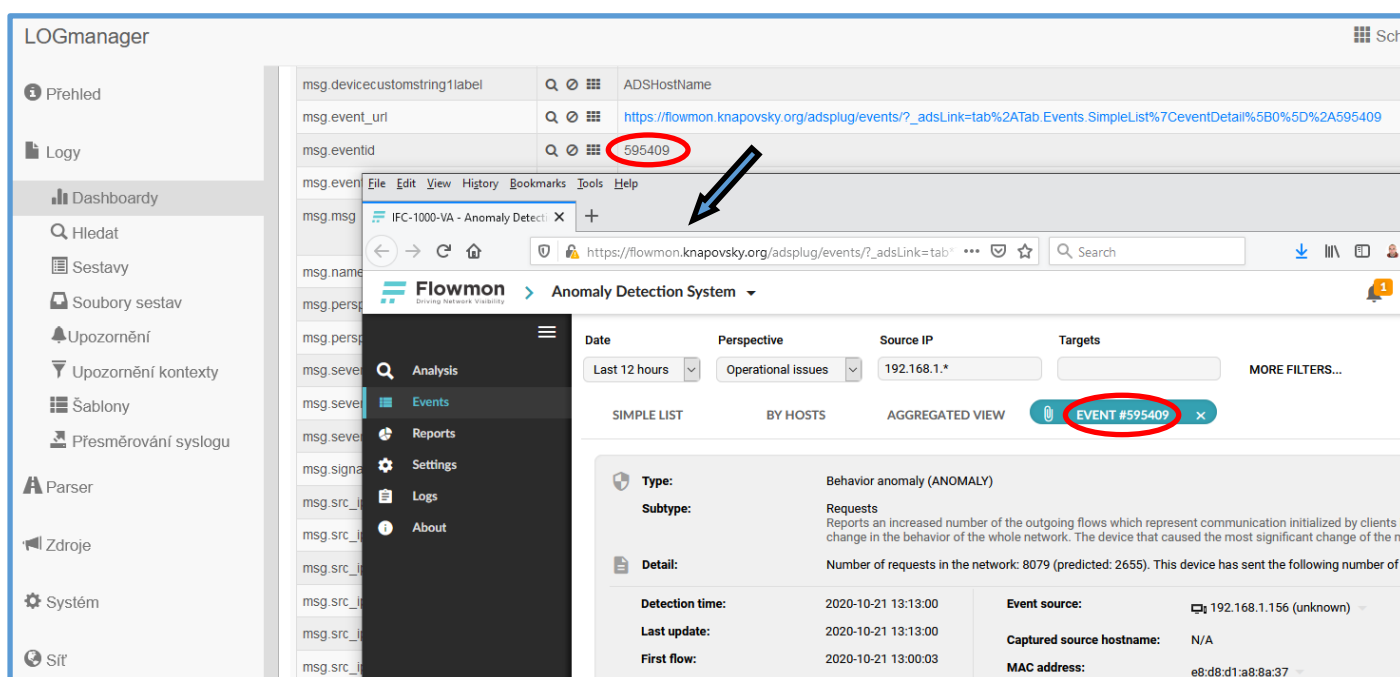
» 2. Obohacení logů Flowmon o dodatečná metadata:

Postup pro obohacení logů Flowmon ADS v LOGmanageru o URL linky jednotlivých událostí:

1. Vytvoření nové akce z připraveného vzoru – v menu *Logy / Upozornění*, na seznamu upozornění klikněte na pravou ikonu - Vytvořit nové z template.
2. Vyberte ze seznamu Modelových příkladů ten s názvem: „Flowmon_log_enhancement“ a klikněte na tlačítko použít.
3. V bloku modelového příkladu editujte pole označené šipkou na obrázku níže. Do pole napište místo „flowmon.local.domain“ doménové jméno nebo IP adresu Vašeho Flowmon systému.



4. Dle potřeby upravte název a popis a upozornění, doplňte email adresu tvůrce upozornění, povolte alert a v posledním kroku klikněte na tlačítko „Vytvořit“. Tím je upozornění, které neupozorňuje, ale doplňuje ke každému Flowmon ADS logu URL hotovo. Do jedné minuty u nově přichozích logů naleznete nové pole msg.event_url.
5. Kontrola výsledku. Otevřete příslušnou událost Flowmon ve vestavěném Dashboardu Flowmon, naleznete pole msg.event_url a otestujte, zda Vás správně přesměruje na danou událost ve Flowmon, tak jako na obrázku níže.



Obrázek: náhled výsledku vytvoření nového pole a provázání

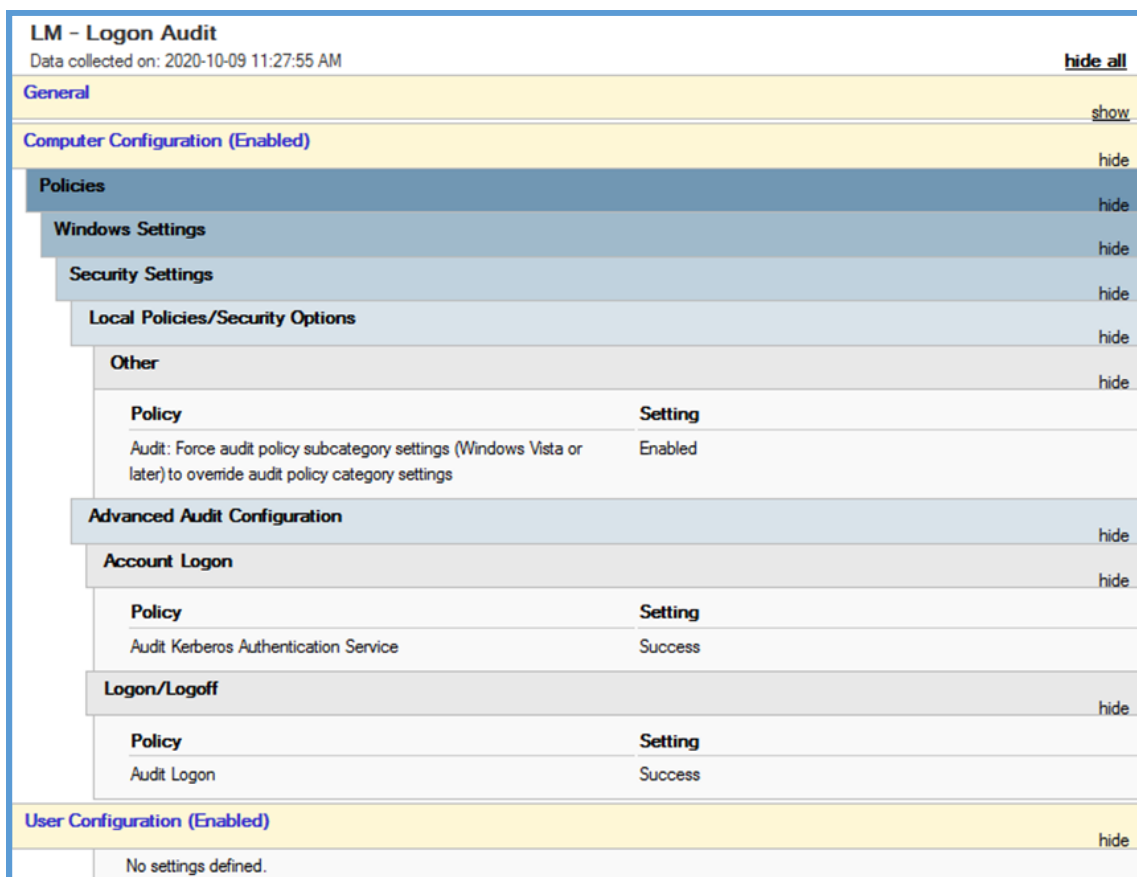
» 3. Doplnění uživatelské identity z LOGmanageru do Flowmon

Základní logika této integrace: LOGmanager může přeposílat události spojené s úspěšným přihlášením uživatele do systému Flowmon. V systému Flowmon je pak možné propojit např. toky dat s identitou konkrétního uživatele. Pro úspěšné propojení identity uživatele s tokem dat je třeba na doménových serverech nastavit logování událostí spojených s ověřením identity (např. přes GPO), tyto události z LOGmanageru přeposílat na Flowmon. Flowmon musí informace o identitě uživatelů přijaté z LOGmanageru musí zpracovat parserem, který jsme pro Vás taktéž připravili a naleznete jej v návodu níže.

1. **Konfigurace GPO:** První je nutné vytvořit skupinovou politiku pojmenovanou např. *LM – Logon Audit* a spojit ji s kontejnerem řadičů domény a ideálně i s kontejnerem členských serverů domény.

Editovat nově vytvořenou skupinovou politiku a v cestě *Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Security Options* změnit politiku *Audit: Force audit policy subcategory settings to override audit policy category settings*, zaškrtnout volbu *Define this policy settings*, volbu *Enabled* a potvrdit tlačítkem OK.

Dále v cestě *Computer Configuration / Policies / Windows Settings / Security Settings / Advanced Audit Policy Configuration / Audit Policies / Account Logon* změnit politiku *Audit Kerberos Authentication Service*, zaškrtnout volbu *Configure the following audit events*, volbu *Success* a potvrdit tlačítkem OK. Nakonec v cestě *Computer Configuration / Policies / Windows Settings / Security Settings / Advanced Audit Policy Configuration / Audit Policies / Logon/Logoff* změnit politiku *Audit Logon*, zaškrtnout volbu *Configure the following audit events*, volbu *Success* a potvrdit tlačítkem OK.



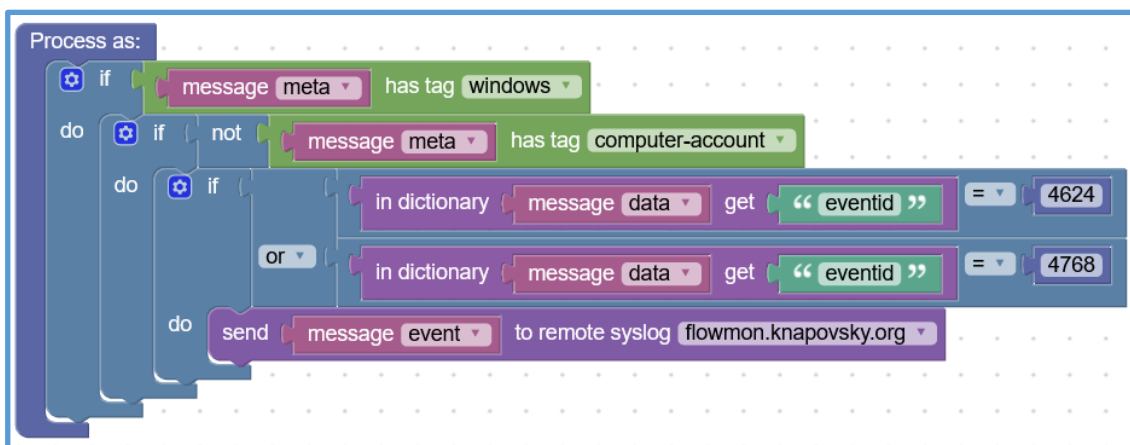
LM - Logon Audit		hide all
Data collected on: 2020-10-09 11:27:55 AM		
General		show
Computer Configuration (Enabled)		hide
Policies		hide
Windows Settings		hide
Security Settings		hide
Local Policies/Security Options		hide
Other		hide
Policy	Setting	
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled	
Advanced Audit Configuration		hide
Account Logon		hide
Policy	Setting	
Audit Kerberos Authentication Service	Success	
Logon/Logoff		hide
Policy	Setting	
Audit Logon	Success	
User Configuration (Enabled)		hide
No settings defined.		

Obrázek: náhled výsledku vytvoření nové auditní politiky v AD

2. **Konfigurace LOGmanager:** Nejprve je třeba definovat nový cíl vybraných logů na Flowmon syslog kolektor. V LOGmanager menu *Logy / Přesměrování syslogu* je třeba přidat nové přesměrování. Do formuláře vyplnit IP adresu a port (výchozí port pro syslog je 514), kde naslouchá Flowmon, do pole *Syslog output message format version* nastavit hodnotu 2 a zaškrtnout volbu *Enabled*. Uložit konfiguraci tlačítkem *Save*. Screenshot vzoru nově vytvořeného záznamu naleznete na další stránce.

Obrázek: náhled vytvoření nového cíle pro odesílání logů

Dále je třeba vytvořit upozornění podle příkladu níže, které bude vybrané auditní události přeposílat na Flowmon. V menu *Logy / Upozornění* přidejte nové upozornění. Do formuláře pro nové upozornění je třeba vyplnit název, případně i popis, do pole cíl vyplňte e-mailovou adresu a zaškrtnout volbu *Enabled*. V poli Blocks vytvořte alert podle následujícího obrázku. V bloku "send to remote syslog" je třeba vybrat přesměrování vytvořené v předchozím kroku. Nakonec konfiguraci uložte tlačítkem Save.



Obrázek: náhled vytvoření bloku upozornění pro odesílání logů

3. **Konfigurace Flowmon:** Ve Flowmon *Configuration center / Systém* na záložce *Nastavení systému* je třeba přidat nový *Syslog server*. Musí být zaškrtnuta volba *Povolit externí protokoly syslog* a pomocí tlačítka *Nový Syslog Client* musí být nastavena informace, odkud budou přicházet události. V tomto případě zde bude IP adresa systému LOGmanager, port 514 (jde o stejný port, který je nastavený v konfiguraci přesměrování v LOGmanageru) a protokol TCP. Dále je třeba zapnout volbu *Povolit parsování informací o identitě uživatelů* a vytvořit dvě nová parsovací pravidla pomocí tlačítka *Nové pravidlo* pro získání informací z událostí 4624 a 4768.

V prvním novém pravidle pro událost 4624 do pole *Název* vyplnit vhodný název (např. Windows Logon 4624) a do pole *Pravidlo pro zprávy o přihlášení* zapsat následující pravidlo:

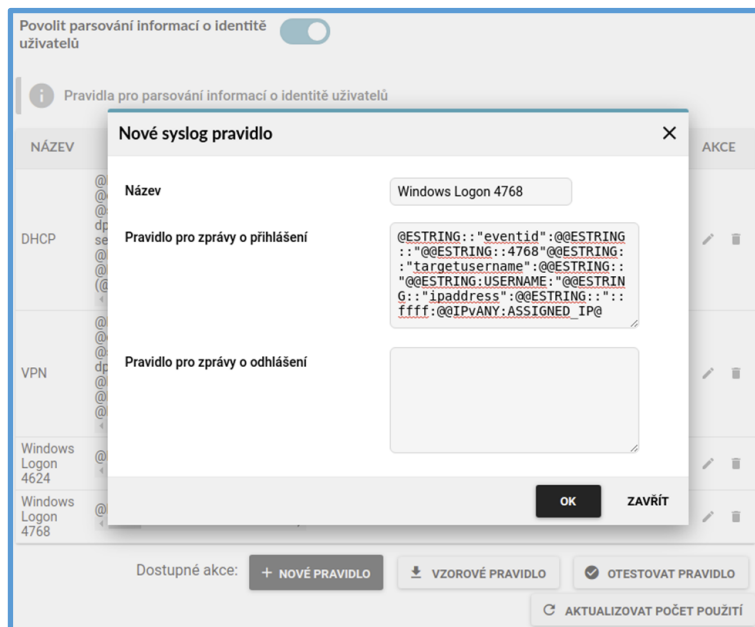
```
@ESTRING::"eventid":@@ESTRING::"@ESTRING::4624"@ESTRING::"targetusername":@@ESTRING::"@ESTRING:USERNAME:"@@ESTRING::"ipaddress":@@ESTRING::"@IPvANY:ASSIGNED_IP@
```

V druhém novém pravidle pro událost 4768 do pole *Název* vyplnit jiný vhodný název (např. Windows Logon 4768) a do pole *Pravidlo pro zprávy o přihlášení* zapsat následující pravidlo:

```
@ESTRING::"eventid":@@ESTRING::"@ESTRING::4768"@ESTRING::"targetusername":@@ESTRING::"@ESTRING:USERNAME:"@@ESTRING::"ipaddress":@@ESTRING::":ffff:@IPvANY:ASSIGNED_IP@
```

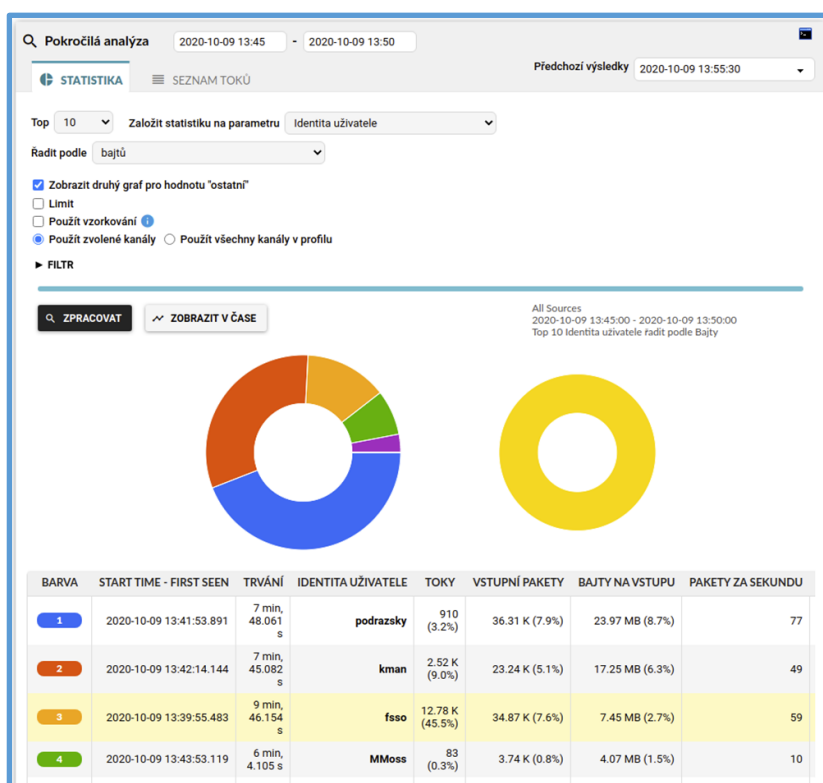
Nakonec je třeba stisknout tlačítko *Uložit* pro uložení konfigurace.

Screenshot vzoru nově vytvořeného záznamu parsovacího pravidla naleznete na další stránce.



Obrázek: náhled vytvoření nového syslog pravidla ve Flowmon

4. **Ověření funkčnosti:** Správnost integrace zpracování identit uživatelů je možné ověřit např. v *Monitoring Center*. V nabídce vybrat možnost *Analýza* a ve spodní části stránky *Pokročilá analýza* vybrat v poli *Založit statistiku na parametru* hodnotu *Identita uživatele*. Poté kliknout na tlačítko *Zpracovat*. Pokud je vše správně, zobrazí se statistika toků dat podle identity uživatelů jako na screenshotu níže.



Návrhy a doporučení k tomuto návodu prosím zasílejte na email adresu: security-team@logmanager.com

INFORMACE O VÝROBCI A DALŠÍ REFERENCE

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovníctví a další. Pro podrobnější list referencí přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.