PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené
ako otvorená cloudová služba s prvkami strojového učenia

Dashboardy – ukážka tvorby vizualizácií v Kibane

Previazané s balíkom KPB2 – Návrh SOCaaS služby

Previazané s výstupom
V6 – Popis dashbordov, monitorovacieho a reportovacieho systému

Obsah

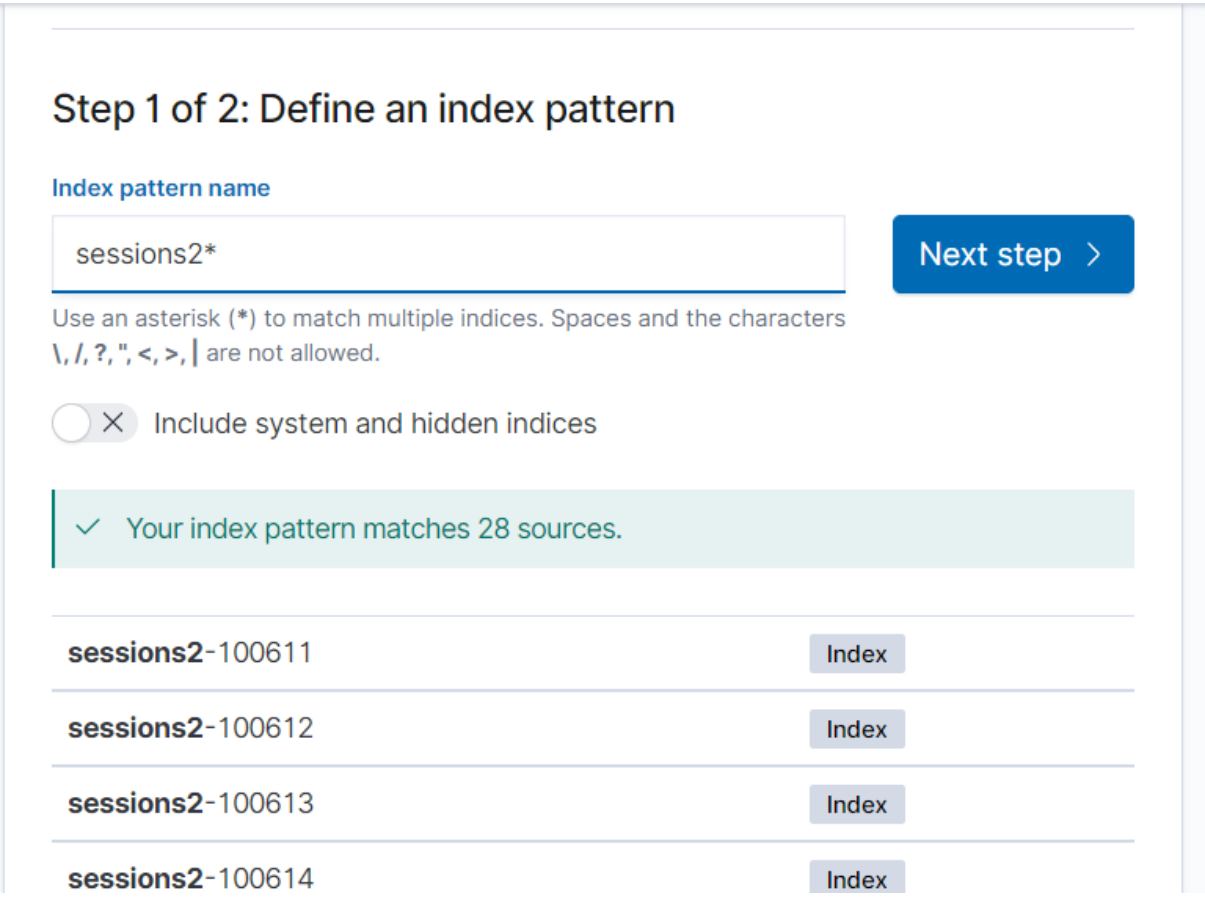
Zoznam obrázkov

Tvorba Kibana dashboardov

V tejto časti dokumentu uvádzame ukážku postupu pri tvorbe vizualizácií a dashboardov, ktorým sme sa venovali.

Indexový vzor (angl. Index pattern)

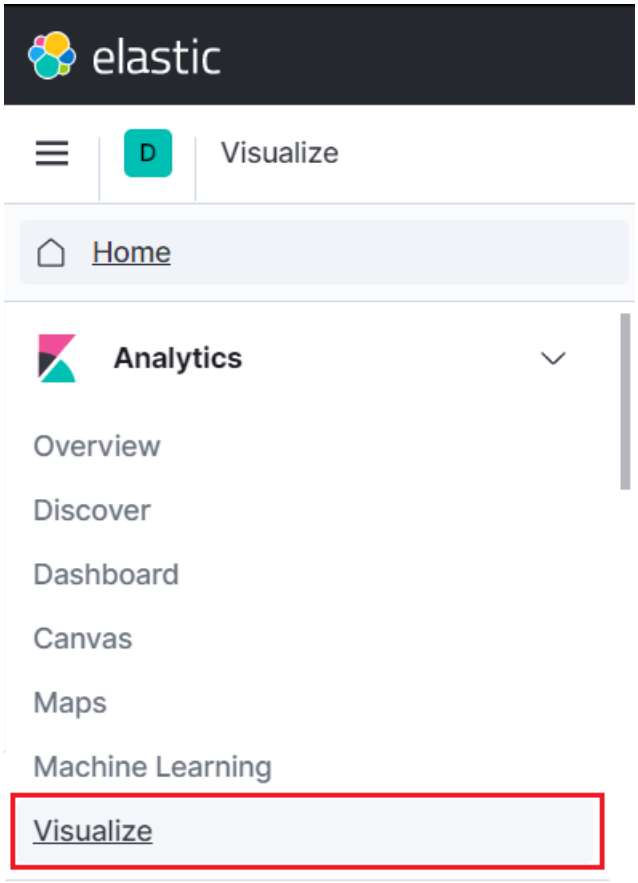
Ako prvé sme si v časti Management/Stack management/Index pattern potrebovali vytvoriť tzv. index pattern z dostupných indexov. Takto vytvorený vzor slúži na určenie indexov, ktoré budú vizualizované. Všetky indexy, ktoré spĺňajú zadaný tvar (v tomto prípade „sessions2*“) budú zahrnuté do tvorených vizualizácií a dashboardov.



Obrázok 1 - Kibana - index pattern

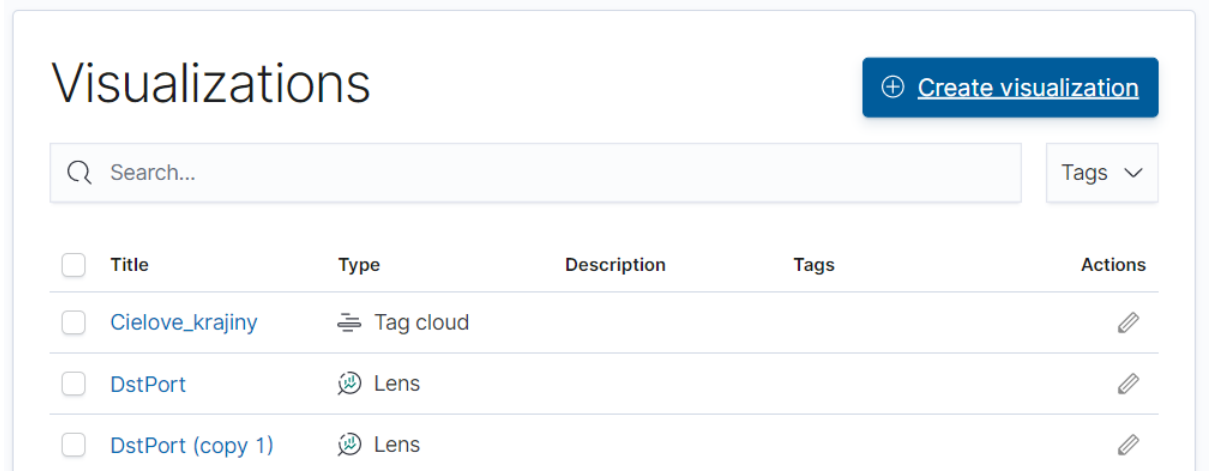
Vizualizácie

Vizualizácie patria k hlavným prvkom dashboardov. Ide o grafické vyobrazenie zvolených dát väčšinou v podobe grafov. Vytvárať sa dajú viacerými spôsobmi, z ktorých jeden si ukážeme v tomto dokumente. V menu Kibany si zvolíme Visualize pod kategóriou Analytics.



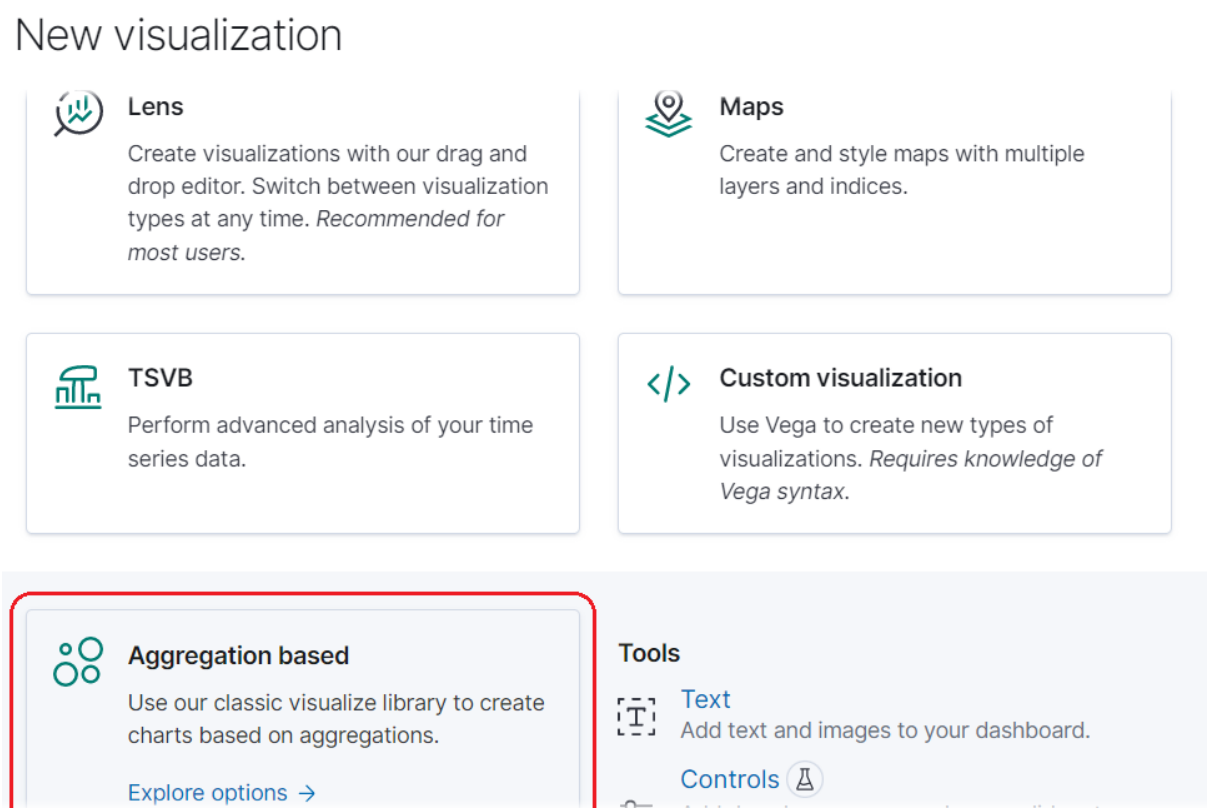
Obrázok 2 - Kibana menu - visualize

Dostaneme sa k zoznamu už vytvorených vizualizácií, kde kliknutím na modré tlačidlo vytvoríme novú vizualizáciu.

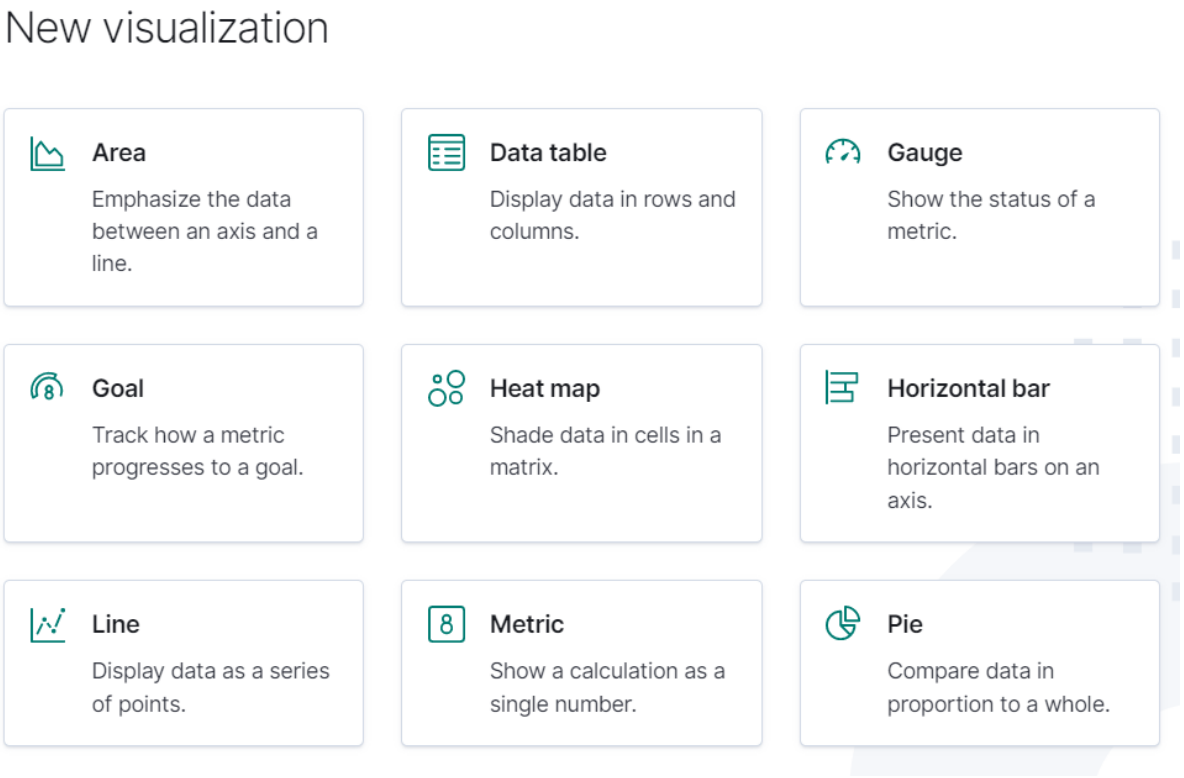


Obrázok 3 - Kibana - zoznam vizualizácií

Následne si zvolíme z možností, ktoré sú k dispozícii. Najčastejšie bola používaná možnosť „Agregation based“, kde sme si ďalej vybrali požadovaný typ grafu.

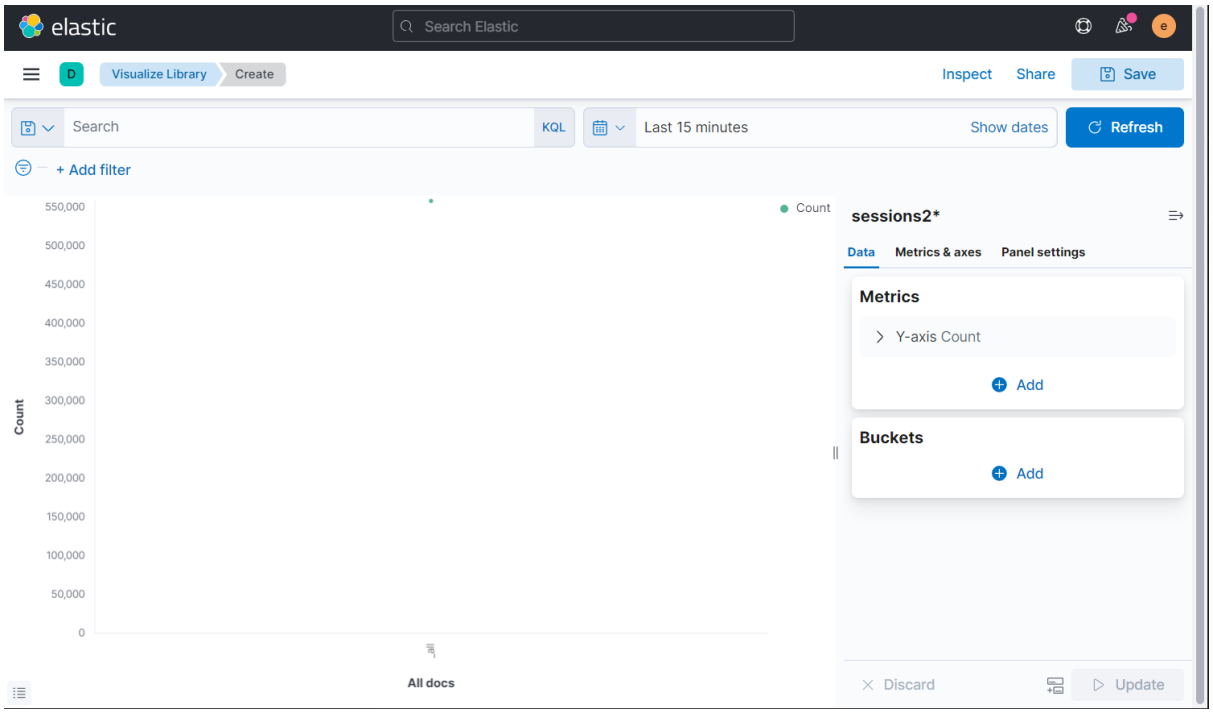


Obrázok 4 - Kibana - voľba vizualizácie



Obrázok 5 - Kibana - voľba grafu

Po týchto voľbách už prechádzame k tvorbe konkrétneho grafu určením osí, metrík, či iných parametrov, ktoré nástroj Kibana ponúka. Už záleží na tom, čo chceme danou vizualizáciou zobraziť. Nižšie na obrázku môžeme vidieť prostredie na tvorbu stĺpcového grafu.



Obrázok 6 - Kibana - tvorba stĺpcového grafu

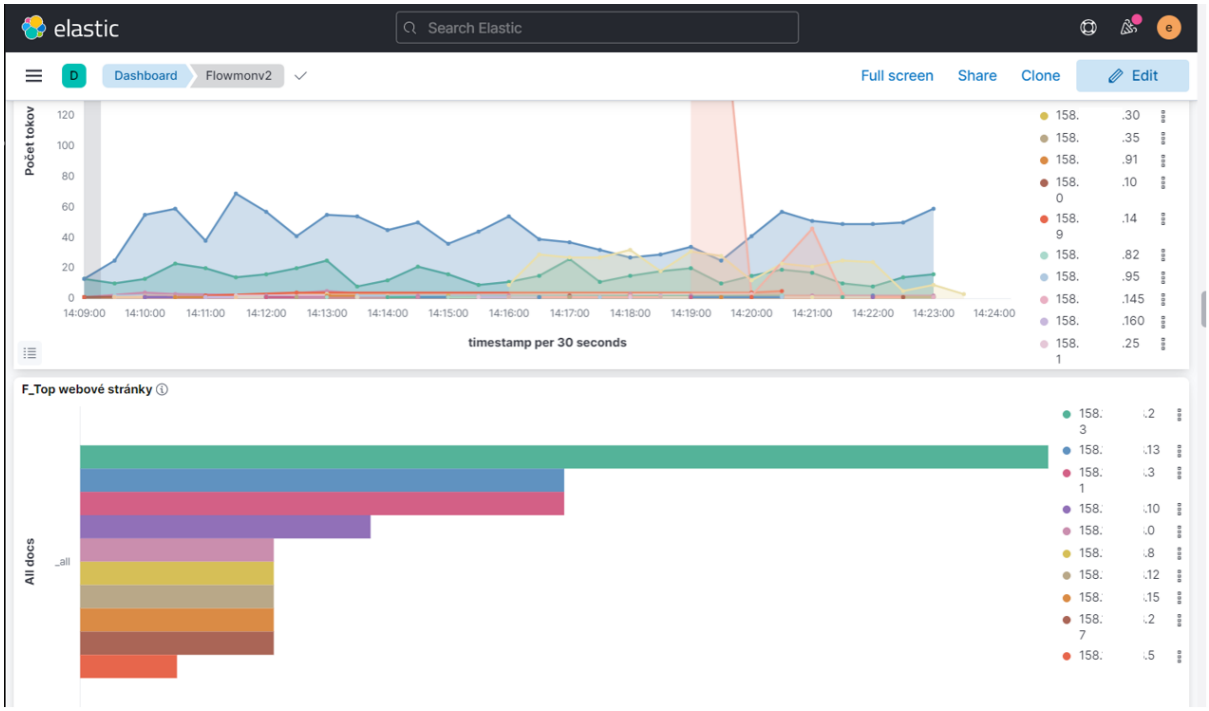
Filtre

Vizualizácie vo všeobecnosti používajú filtre, ktoré bližšie špecifikujú na akú časť záznamov sa majú sústrediť. Či už ide o špecifické IP adresy, porty alebo protokoly, v našom prípade boli použité filtre, ktoré sa nachádzajú v závere tohto dokumentu.

Príklad: dstIp : "<IPadresa>" or dstIp : "<IPadresa>" "

Dashboard

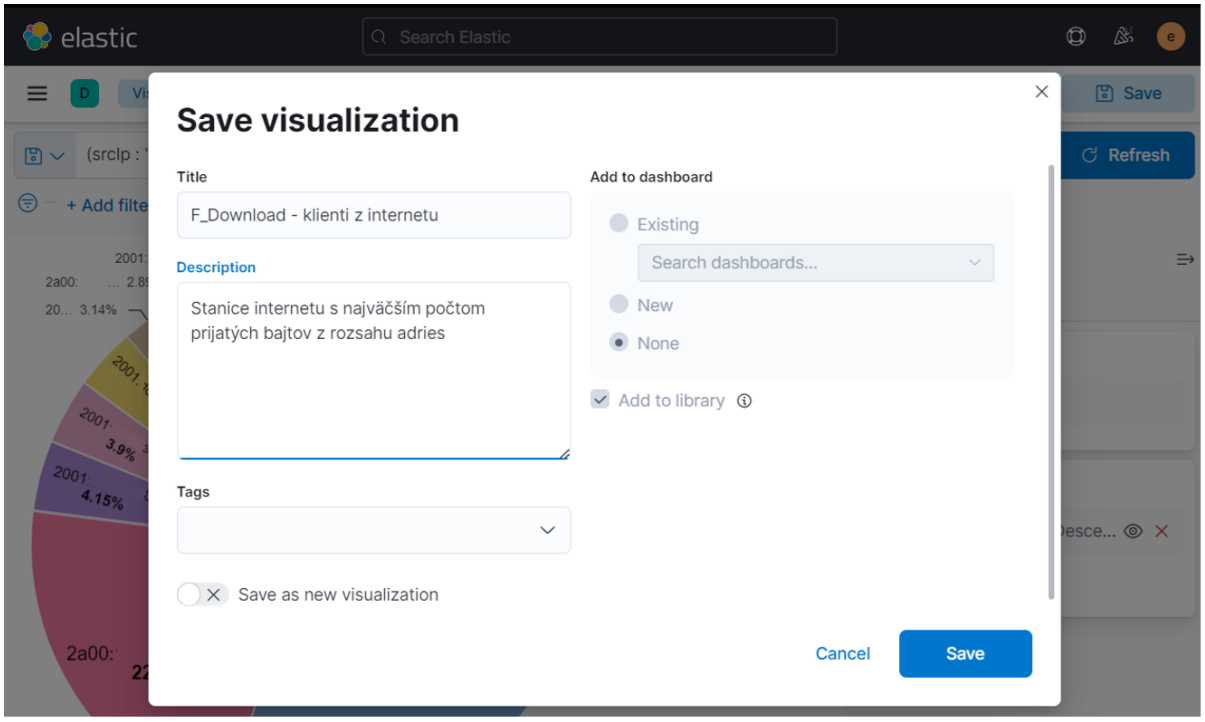
Tvorba dashboardu samotného spočíva vo vkladaní vizualizácií do určeného priestoru. Tieto vizualizácie môžeme vkladať v ľubovoľnom poradí, presúvať ich, či meniť ich veľkosť presne podľa našej potreby. Takýmto štýlom si vieme naskladať všetky potrebné vizualizácie na jedno miesto a tým si uľahčiť prácu. Výsledný vzhľad dashboardov závisí od preferencií analytika, či požiadavkách centra, respektíve organizácie.



Obrázok 7 - Kibana - dashboard príklad

Popis vizualizácií

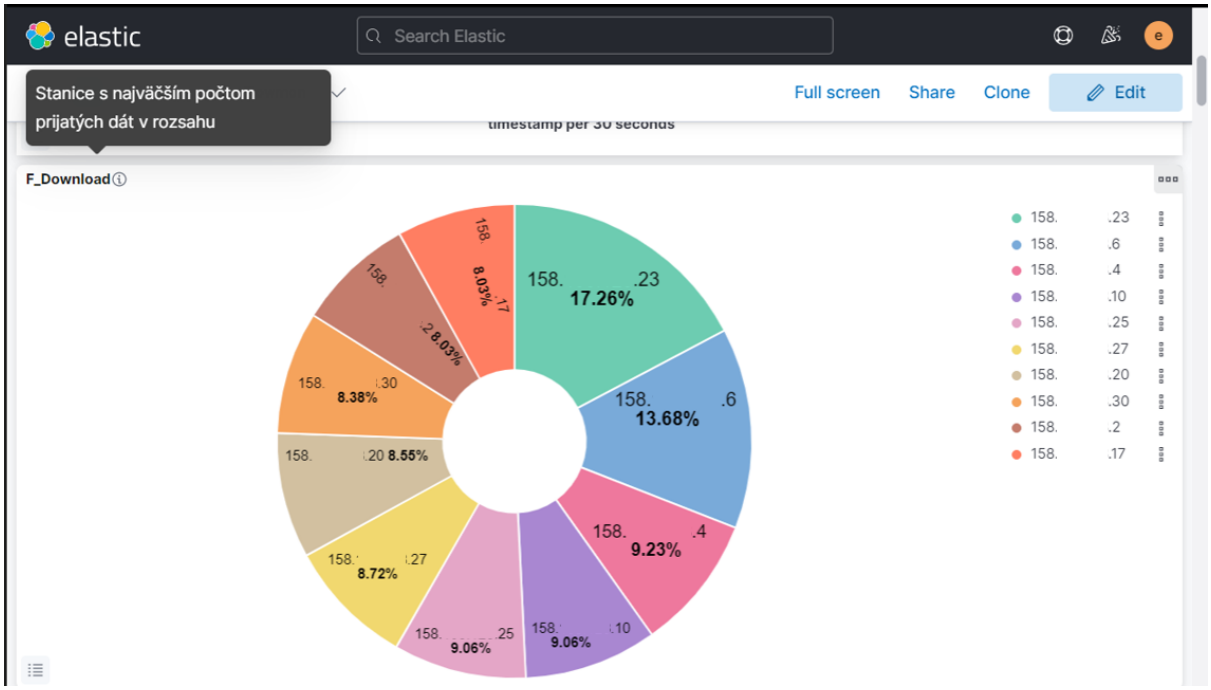
Slúži najmä pre lepšie pochopenie konkrétnej vizualizácie, pretože niekedy na prvý pohľad nie je známe, čo sa daná vizualizácia snaží vyjadriť. Najmä ak človek nahliada do dashboardov prvý raz. Spôsob ako tieto popisy pridať je zobrazený na obrázku nižšie. Popis sa pridáva priamo pri vytváraní vizualizácie, respektíve pri jej ukladaní. Takisto ak už vizualizácia bola vytvorená, po jej otvorení máme možnosť kliknúť na tlačidlo „Save“ aj bez vykonaných zmien a popis vložiť do príslušnej časti.



Obrázok 8 - Kibana - pridanie popisu vizualizácie

Pridanie popisu vizualizácie

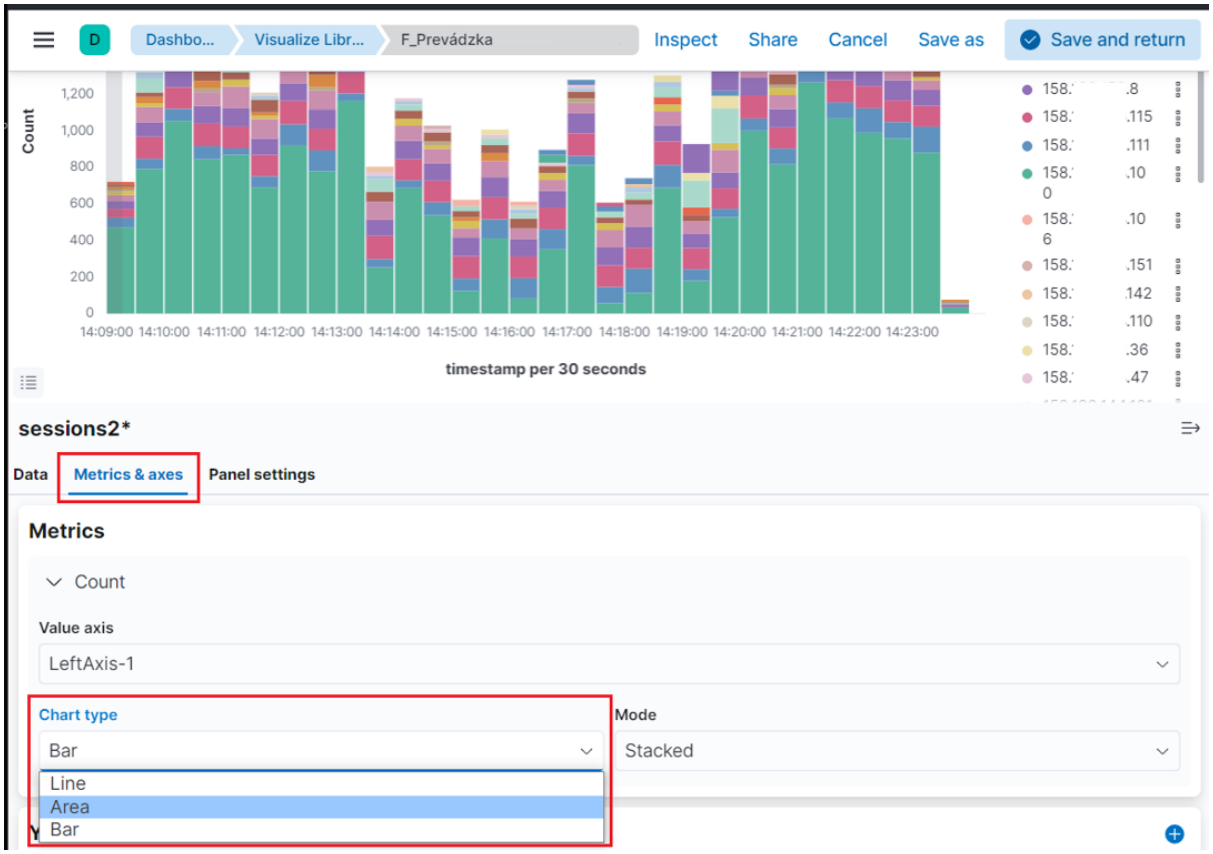
Popis sa nám zobrazí priamo v zozname vytvorených vizualizácií. Rovnako tak je však viditeľný aj priamo v dashboardoch, kde vedľa názvu vizualizácie môžeme vidieť drobnú ikonku „?“ , na ktorú keď prejdeme myšou, zobrazí daný popis v pop-up bubline, ktorú môžeme vidieť na obrázku nižšie.



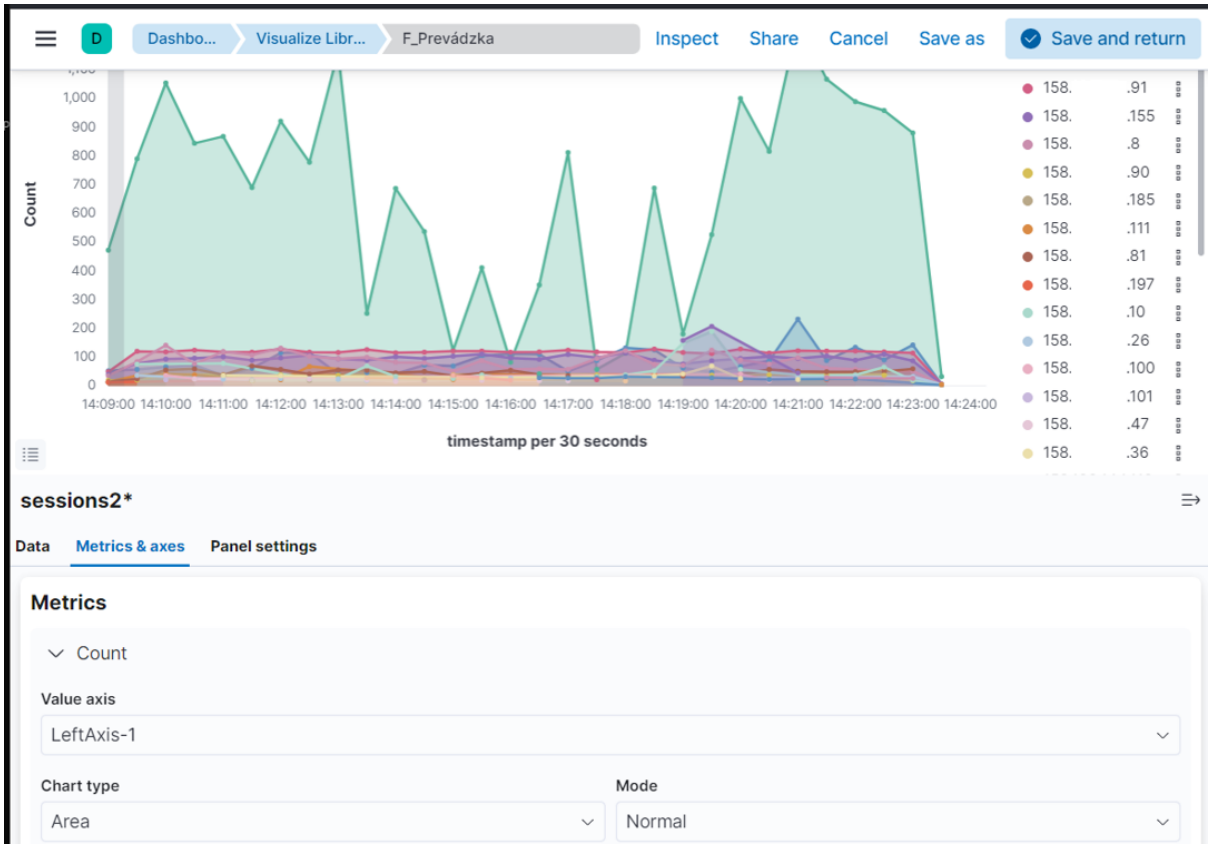
Obrázok 9 - Kibana - zobrazenie popisu v dashboarde

Zmena typu grafu

Pri bežnej tvorbe grafu, ako je popísaná vyššie nastáva problém pri zmene typu grafu. Čo sa týka zmeny stĺpcových grafov, zmena je možná na čiarový alebo plošný graf. Túto zmenu môžeme vykonať na karte „Matrics & axes“ a prepnúť „chart type“ na požadovaný typ. Priebeh zmeny a jej výsledok môžeme vidieť na nasledujúcej strane.



Obrázok 10 - Kibana - Zmena typu grafu



Obrázok 11 - Kibana - Graf po zmene

Zoznam použitých filtrov

1. F_CelkovaPrevadzka
-
2. F_Download
dstIp : "158.***.***.0/27" or dstIp : "2001:***:***::0/48"
3. F_Upload
srcIp : "158.***.***.0/27" or srcIp : "2001:***:***::0/48"
4. F_Download - klienti z internetu
(srcIp : "158.***.***.0/27" or srcIp : "2001:***:***::0/48") and (NOT dstIp : "158.***.***.0/27" or NOT dstIp : "2001:***:***::0/48")
5. F_Upload - klienti z internetu
(NOT srcIp : "158.***.***.0/27" or NOT srcIp : "2001:***:***::0/48") and (dstIp : "158.***.***.0/27" or dstIp : "2001:***:***::0/48")
6. F_Servisna prevádzka (sieťové aplikačné služby)
(protocol : "tcp" or protocol : "udp") and (
(dstPort : 161 or dstPort : 162) or
(dstPort : 25 or dstPort : 587 or dstPort : 465 or dstPort : 2525) or
(dstPort : 53) or
(dstPort : 67 or dstPort : 68) or
(dstPort : 445 or dstPort : 139) or
(dstPort : 23)
)
7. F_Smerovacie protokoly ***
protocol :"gre"
8. F_Prevádzky
(dstIp : "158.***. ***.0/24" or dstIp : "158.***. ***.0/24" or dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24" or dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24" or dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***.***.0/24" or dstIp : "158.***. ***.0/24")
9. F_Prevádzka podľa laboratorií
(srcIp : "158.***. ***.0/24") or
(srcIp : "158.***. ***.0/24") or
(srcIp : "158.***. ***.0/24") or
(srcIp : "158.***. ***.0/24") or
(srcIp : "158.***. ***.0/24")
10. F_Top webové stránky
(dstIp : "158.***.***.0/27" or dstIp : "2001:***:***::0/48") and (dstPort : 80 or dstPort : 443)

11. F_Top webové stránky - Internet
(NOT dstIp : "158.***.***.0/27" or NOT dstIp : "2001:***:***::0/48") and (dstPort : 80 or dstPort : 443)
12. F_Top webové servery - Intranet
(srcPort : 80 or srcPort : 443) and (protocol : "tcp") and (srcIp : "158.***.***.0/27" or srcIp : "2001:***:***::0/48")
13. F_Top webové servery - Internet
(srcPort : 80 or srcPort : 443) and (protocol : "tcp") and (NOT srcIp : "158.***.***.0/27" or NOT srcIp : "2001:***:***::0/48")
14. F_TCP služby
protocol : tcp and srcIp : "158.***.***.0/27" and srcPort < 49151
15. F_UDP služby
protocol : "udp" and srcIp : "158.***.***.0/27" and srcPort < 49151
16. F_Poštová prevádzka
(srcPort : 110 or srcPort : 995) or
(srcPort : 143 or srcPort : 993) or
(srcPort : 25 or srcPort : 587 or srcPort : 465 or srcPort : 2525)
17. F_Stanice s najvyšším množstvom tokov
srcIp : "158.***.***.0/27" or srcIp : "2001:***:***::0/48"
18. F_Stanice s najvyšším množstvom tokov - Internet
NOTsrcIp : "158.***.0.0/16" or NOT srcIp : "2001:***:***::0/48"
19. F_Top odosielatelia pošty a SMTP servery
(protocol : "tcp" or protocol : "udp") and (srcPort : 25 or srcPort : 587 or srcPort : 465 or srcPort : 2525)
20. F_Top používateľia pošty a POP3/IMAP servery
(srcPort : 110 or srcPort : 995) or
(srcPort : 143 or srcPort : 993)
21. F_Downlad – Cloud2
dstIp : "158.***. ***.0/24" or dstIp : "2001:***:***:124::/64"
22. F_Upload – cloud2
NOT srcIp : "158.***. ***.0/24"
23. F_Upload - labs2
srcIp : "158.***. ***.0/24" or srcIp : "158.***. ***.128/25"
24. F_Download - labs2
dstIp : 158.***. ***.0/24 or srcIp : 158.***. ***.128/25