STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Monitor siete**

**Juraj Petrina**

2024

Obsah

Obsah 2

Anotácia 3

1 Prometheus 5

1.1 Popis 5

1.2 Dôvody výberu 5

1.3 Funkčnosť 6

1.4 História 6

1.5 Vlastnosti 7

1.6 Architektúra 7

2 Grafana 8

2.1 Popis 8

2.2 Dôvody výberu 8

2.3 História 8

2.4 Vlastnosti 9

3 SNMP 10

3.1 Popis 10

3.2 Architektúra 10

3.3 Verzie SNMP protokolu 10

3.4 Funkčnosť 10

4 Prepojenie 12

4.1 Čo je SNMP Exporter? 12

4.2 Nastavenie exportéra SNMP: 12

4.3 Integrácia s Prometheus: 12

4.4 Vizualizácia údajov pomocou Grafany: 13

4.5 Výhody integrácie: 13

5 Záver 15

Zoznam použitej literatúry 16

Anotácia

Tento projekt sa zaoberá vytvorením sieťového monitoru s vizualizáciou na osobnom počítači s využitím nástrojov Prometheus, SNMP (SNMP\_Exporter) a Grafana. Cieľom projektu je sledovanie sieťového prevozu, analýza dát a vizualizácia v reálnom čase pomocou interaktívnych grafov a panelov.

Na začiatku projektu bol nainštalovaný a konfigurovaný nástroj SNMP\_Exporter na sledovanie sieťového prevozu. Pomocou neho boli zachytávané dáta, ktoré následne slúžili ako vstup pre monitorovanie a vizualizáciu.

Potom bol nainštalovaný a konfigurovaný nástroj Prometheus, ktorý slúžil na ukladanie (databáza), monitorovanie a spravovanie dát. Prometheus bol pripojený k SNMP\_Exporteru a zachytával dáta.

Následne bol nainštalovaný a konfigurovaný nástroj Grafana, ktorý slúžil na vizualizáciu sieťového prevozu. Grafana bola pripojená k databáze (Prometheus) zachytávaných dát a umožňovala vytváranie interaktívnych grafov a panelov na základe týchto dát.

Po nastavení bolo nastavené periodické meranie sieťového prevozu a zabezpečenie nástrojov Prometheus, SNMP\_Exporter a Grafana.

Výsledkom projektu je funkčný sieťový monitor s vizualizáciou, ktorý umožňuje sledovať a analyzovať sieťový prevoz a detekovať potenciálne problémy v reálnom čase.

**Annotation**

This project deals with the creation of a network monitor with visualization on a personal computer using Prometheus, SNMP (SNMP\_Exporter) and Grafana tools. The goal of the project is monitoring of network traffic, data analysis and visualization in real time using interactive graphs and panels.

At the beginning of the project, the SNMP\_Exporter tool was installed and configured to monitor network traffic. With the help of which data was captured, which subsequently served as input for monitoring and visualization.

Then the Prometheus tool was installed and configured, which was used for storing (database), monitoring and managing data. Prometheus was connected to SNMP\_Exporter and was capturing data.

Subsequently, the Grafana tool was installed and configured, which was used to visualize the network transport. Grafana was connected to the database (Prometheus) of captured data and enabled the creation of interactive graphs and panels based on this data.

After the setup, the periodic interference of the network transport and the security of the Prometheus, SNMP\_Exporter and Grafana tools were set.

The result of the project is a functional network monitor with visualization that allows you to monitor and analyze network traffic and detect potential problems in real time.

1. Prometheus
   1. Popis

Prometheus je bezplatná softvérová aplikácia používaná na monitorovanie a upozorňovanie udalostí. Zaznamenáva metriky do databázy časových radov (umožňujúce vysokú dimenzionalitu) vytvorenej pomocou modelu ťahania HTTP s flexibilnými dopytmi a varovaním v reálnom čase. Prometheus je napísaný v Go a licencovaný pod licenciou Apache 2 License, so zdrojovým kódom dostupným na GitHub, a je to absolventský projekt Cloud Native Computing Foundation spolu s Kubernetes a Envoy.

* 1. Dôvody výberu
* Flexibilita a rozšíriteľnosť: Prometheus poskytuje široké možnosti konfigurácie a prispôsobenia, čo umožňuje monitorovať rôzne aspekty siete a ľahko pridávať nové metriky podľa potreby. Táto flexibilita je kľúčová pre efektívne sledovanie rastúcich a komplexných sietí.
* Vysoký výkon a efektivita: Prometheus je navrhnutý na efektívne spracovanie a ukladanie veľkého množstva dát, čo z neho robí ideálnu voľbu pre monitorovanie rozsiahlych sietí. Jeho schopnosť efektívne spracovávať dáta z rôznych zdrojov umožňuje získavanie relevantných informácií bez značného zaťaženia siete.
* Integrácia s Grafanou: Jednou z najväčších výhod je možnosť jednoduchej integrácie s Grafanou, populárnym nástrojom na vizualizáciu dát. Táto integrácia umožňuje ľahké vytváranie vizuálnych prezentácií monitorovaných údajov, čo zlepšuje prehľadnosť a zrozumiteľnosť pre užívateľov.

Nevýhody:

* Komplexita správy: Aj keď je Prometheus vynikajúci nástroj pre monitorovanie siete a poskytuje množstvo výhod, jeho implementácia a správa môže byť pomerne zložitá. Konfigurácia a údržba tohto nástroja vyžaduje určitú technickú znalosť a investíciu času, čo môže byť pre niektoré organizácie náročné.
  1. Funkčnosť

Prometheusu spočíva v jeho schopnostiach monitorovať a zbierať dáta z rôznych zdrojov v sieti, analyzovať tieto dáta a poskytovať užitočné informácie o stave a výkone systému. Hlavné funkcie Prometheusu zahŕňajú:

1. **Zber dát**: Prometheus dokáže zbierať dáta pomocou rôznych metód, ako sú HTTP, HTTPS, SNMP, DNS alebo aj vlastné exporty aplikácií. Tieto dáta môžu byť ľahko získané z rôznych zdrojov v sieti.
2. **Ukladanie dát**: Zozbierané dáta sú ukladané do lokálnej databázy s časovými značkami, čo umožňuje históriu a retrospektívnu analýzu.
3. **Dotazovanie a vyhľadávanie dát**: Používatelia môžu vykonávať dotazy nad uloženými dátami pomocou dotazovacieho jazyka PromQL, ktorý umožňuje vyhľadávanie a agregáciu údajov podľa rôznych kritérií.
4. **Alertovanie**: Prometheus umožňuje definovať pravidlá pre výstrahy na základe špecifikovaných podmienok alebo prahu hodnôt. To umožňuje identifikovať problémy a reagovať na ne v reálnom čase.
5. **Integrácia s ďalšími nástrojmi**: Prometheus je ľahko integrovateľný s ďalšími nástrojmi, ako je napríklad Grafana, na vizualizáciu dát, ale aj s nástrojmi na logovanie, sledovanie kontajnerov a inými.
   1. História

Prometheus bol vyvinutý v SoundCloud od roku 2012, keď spoločnosť zistila, že jej existujúce metriky a monitorovacie nástroje (pomocou StatsD a Graphite) nepostačujú pre ich potreby. Konkrétne identifikovali potreby, pre ktoré bol Prometheus vytvorený, vrátane viacrozmerného dátového modelu, prevádzkovej jednoduchosti, škálovateľného zberu dát a výkonného dotazovacieho jazyka, a to všetko v jedinom nástroji. Projekt bol od začiatku open-source a začali ho využívať aj používatelia Boxeveru a Dockeru, napriek tomu, že to nebolo výslovne oznámené. Prometheus sa inšpiroval monitorovacím nástrojom Borgmon používaným v Google.

V máji 2016 Cloud Native Computing Foundation prijala Prometheus ako svoj druhý inkubovaný projekt po Kubernetes. V blogovom príspevku, ktorý to oznamoval, sa uvádzalo, že tento nástroj sa používa v mnohých spoločnostiach vrátane DigitalOcean, Ericsson, CoreOS, Weaveworks, Red Hat a Google.

* 1. Vlastnosti

Hlavné vlastnosti Prometheusu sú:

* viacrozmerný dátový model s údajmi časových radov identifikovaných názvom metriky a pármi kľúč/hodnota
* PromQL, flexibilný dopytovací jazyk na využitie tejto dimenzie
* žiadne spoliehanie sa na distribuované úložisko; jednotlivé uzly servera sú autonómne
* Zhromažďovanie časových radov prebieha prostredníctvom modelu pull cez HTTP
* tlačenie časových radov je podporované cez sprostredkovateľskú bránu
* ciele sa zisťujú prostredníctvom zisťovania služby alebo statickej konfigurácie
* podpora viacerých režimov grafov a dashboardov
  1. Architektúra
* Model založený na ťahu: Prometheus funguje na modeli založenom na ťahu, kde pravidelne scrapuje metriky z nakonfigurovaných cieľov. Tento model zjednodušuje nastavenie a zaisťuje efektívny zber údajov, čo umožňuje spoločnosti Prometheus jednoducho škálovať v rôznych prostrediach.
* Databáza časových sérií: Prometheus ukladá zhromaždené metriky do databázy časových sérií, čo umožňuje rýchle a efektívne vyhľadávanie historických údajov. Každý časový rad predstavuje jedinečnú metriku s priradenými štítkami, čo umožňuje flexibilnú analýzu a vizualizáciu metrík v priebehu času.
* PromQL: Prometheus Query Language (PromQL) umožňuje používateľom vykonávať výkonné dotazy na zhromaždené údaje metrík. PromQL podporuje agregáciu, filtrovanie a matematické operácie, čo používateľom umožňuje získavať cenné poznatky a vytvárať prispôsobené dashboardy na monitorovanie a analýzu.

1. Grafana
   1. Popis

Grafana je open-source platforma pre vizualizáciu dát a monitorovanie. Umožňuje vytváranie interaktívnych grafov, panelov a dashboardov na základe dát z rôznych zdrojov.

* 1. Dôvody výberu
* Flexibilita: Grafana podporuje mnoho rôznych typov databáz a zdrojov dát, čo umožňuje jednoduchú integráciu s rôznymi systémami a nástrojmi.
* Vizuálna atraktivita: Grafana poskytuje širokú škálu vizualizačných možností, vrátane grafov, tabuliek, panelov a dashboardov, ktoré je možné ľahko prispôsobiť podľa potrieb užívateľa.
* Široká podpora komunity: Grafana má veľkú a aktívnu komunitu užívateľov, čo znamená, že je ľahké nájsť pomoc, tutoriály a rozšírenie.

Nevýhody:

* Zložitejšie nastavenia: Nastavenie Grafany môže byť zložitejšie, najmä pri integrácii s niektorými typmi databáz.
  1. História

Grafana bola prvýkrát vydaná v roku 2014 Torkelom Ödegaardom ako odnož projektu na Orbitz. Zamerala sa na databázy časových radov, ako sú InfluxDB, OpenTSDB a Prometheus, ale vyvinula sa na podporu relačných databáz, ako sú MySQL, PostgreSQL a Microsoft SQL Server.

V roku 2019 spoločnosť Grafana Labs zabezpečila financovanie série A vo výške 24 miliónov dolárov. V kole financovania série B v roku 2020 získala 50 miliónov dolárov. V kole financovania Labs Series C v roku 2021 Grafana zabezpečila 220 miliónov dolárov.

* 1. Vlastnosti
* Prispôsobiteľné ovládacie panely: Grafana umožňuje používateľom vytvárať prispôsobené ovládacie panely s rôznymi panelmi, ako sú grafy, tabuľky a meradlá, čo umožňuje efektívnu vizualizáciu údajov.
* Integrácia zdrojov údajov: Grafana sa bezproblémovo integruje s viacerými zdrojmi údajov, ako sú Prometheus, Graphite a Elasticsearch, čím poskytuje jednotný pohľad na systémové metriky.
* Možnosti vizualizácie: Používatelia si môžu vybrať zo širokej škály možností vizualizácie vrátane čiarových grafov, stĺpcových grafov a tepelných máp, ktoré umožňujú jasnú reprezentáciu dátových trendov a vzorov.
* Upozornenia a upozornenia: Grafana ponúka robustné funkcie upozornení, ktoré používateľom umožňujú nastaviť pravidlá upozornenia na základe vopred definovaných prahových hodnôt a prijímať upozornenia prostredníctvom e-mailu, Slacku alebo iných kanálov.
* Používateľské oprávnenia a roly: Administrátori môžu definovať roly a oprávnenia na riadenie prístupu k dashboardom a zdrojom údajov, čím sa zabezpečí bezpečnosť údajov a súlad s organizačnými zásadami.

Tab. 1 Graf inputov v Grafane

A screenshot of a computer

Description automatically generated

1. SNMP
   1. Popis

Jednoduchý manažérsky protokol siete alebo jednoduchý protokol manažérstva siete (angl. Simple Network Management Protocol), skr. SNMP, je protokol umožňujúci monitorovanie a správu zariadení v IP sieti. Primárne bol navrhnutý pre účely správy siete a týkal sa základných sieťových prvkov, napr. smerovačov čomu zodpovedala štandardná MIB báza. Protokol sa však nakoniec uplatnil aj pri správe a monitorovaní ďalších zariadení pripojených v sieti, napríklad sieťových tlačiarní, serverov či koncových užívateľských staníc

* 1. Architektúra

Architektúra SNMP rozoznáva prinajmenšom 2 komponenty:

* Spravovaný objekt (SNMP agent, napr. na prepínači)
* Spravovacia stanica (napr. SNMP platforma)
* Môže obsahovať subagentov (slave).
  1. Verzie SNMP protokolu

SNMPv1

Prvá verzia SNMP protokolu bola definovaná v roku 1988

SNMPv2

Verzia 2 SNMP protokolu sa snažila odstrániť nedostatky SNMPv1. Vzniklo mnoho jej odnoží ktoré riešili bezpečnosť a rozšírenia protokolu. Nakoniec sa stala prakticky štandardom SNMP v2c

SNMPv3

Internet Engineering Task Force (IETF) ustanovuje od roku 2004 verziu SNMPv3

* 1. Funkčnosť
* Kolekcia metrík: SNMP umožňuje zhromažďovať rôzne metriky zo sieťových zariadení, vrátane využitia CPU, pamäte, prenosu rozhrania a chybovosti, čím poskytuje cenné informácie o výkone a stave zariadenia.
* Správa konfigurácie: SNMP umožňuje načítanie a úpravu nastavení konfigurácie zariadení, čím uľahčuje centralizovanú správu a konfiguráciu sieťových zariadení z jedného systému správy.
* Upozorňovanie na udalosti: SNMP podporuje komunikáciu riadenú udalosťami prostredníctvom pascí a informovaní, čo umožňuje zariadeniam odosielať upozornenia do centrálneho riadiaceho systému, keď nastanú špecifické udalosti alebo podmienky, ako sú zmeny stavu spojenia alebo systémové chyby.
* Vzdialená diagnostika: SNMP umožňuje vzdialenú diagnostiku poskytovaním prístupu k diagnostickým informáciám a štatistikám zariadení, čo umožňuje správcom riešiť problémy a identifikovať problémy bez fyzického prístupu k zariadeniu.
* Monitorovanie výkonu: SNMP uľahčuje monitorovanie výkonu sieťových zariadení v reálnom čase, čo umožňuje správcom sledovať trendy, analyzovať historické údaje a zisťovať anomálie s cieľom optimalizovať výkon siete a využitie zdrojov.

A screen shot of a computer

Description automatically generated

Obr. 1 Grafická ukážka SNMP

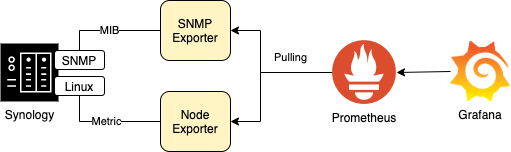
1. Prepojenie

Táto integrácia je kľúčová pre efektívne zhromažďovanie, ukladanie a vizualizáciu metrík výkonu siete.

* 1. Čo je SNMP Exporter?

SNMP Exporter je nástroj, ktorý umožňuje monitorovať sieťové zariadenia a získavať dáta pomocou protokolu SNMP (Simple Network Management Protocol). SNMP Exporter priamo komunikuje so sieťovými zariadeniami, ako sú routery, prepínače a servery, a zbiera dôležité informácie o ich prevádzke, ako sú štatistiky o sieťovom toku, stav rozhraní a ďalšie.

* 1. Nastavenie exportéra SNMP:
* Inštalácia: Začnite inštaláciou nástroja SNMP Exporter na server alebo počítač vo vašej sieti. Tento nástroj funguje ako most medzi zariadeniami s podporou SNMP a Prometheus. SNMP Exporter si môžete stiahnuť z oficiálneho úložiska GitHub.
* Konfigurácia: Po inštalácii nakonfigurujte SNMP Exporter zadaním reťazcov komunity SNMP a cieľových zariadení. Tieto reťazce komunity fungujú ako heslá pre prístup SNMP k zariadeniam. Definujte zariadenia, ktoré chcete monitorovať, vrátane smerovačov, prepínačov, serverov a iných sieťových zariadení.
* Testovanie: Po konfigurácii vykonajte test zoškrabania, aby ste sa uistili, že SNMP Exporter správne získava metriky z cieľových zariadení. Môžete to urobiť pomocou binárneho programu SNMP Exporter a špecifikovaním cieľových adries IP vašich zariadení.
  1. Integrácia s Prometheus:
* Konfigurácia Prometheus: Ďalej integrujte SNMP Exporter s Prometheus, základným komponentom zodpovedným za zhromažďovanie a ukladanie metrík. V konfiguračnom súbore Prometheus (prometheus.yml) definujte novú úlohu na zoškrabovanie koncových bodov exportéra SNMP. Zadajte cieľové koncové body (IP adresu a port), na ktorých je spustený SNMP Exporter.
* Zisťovanie služby: Voliteľne môžete využiť mechanizmy zisťovania služieb Prometheus na dynamické zisťovanie inštancií exportéra SNMP spustených vo vašej sieti. To môže zjednodušiť konfiguráciu a monitorovanie škálovania, keď sa vaša sieť rozrastá.
* Interval scapovania: Nakonfigurujte interval scrapovania v Prometheus, aby ste určili, ako často sa majú metriky zhromažďovať z nástroja SNMP Exporter. Tento interval závisí od vašich požiadaviek na monitorovanie a požadovanej granularity zberu údajov.
  1. Vizualizácia údajov pomocou Grafany:
* Nastavenie Grafany: Keď Prometheus zhromažďuje metriky, posledným krokom je vizualizácia týchto údajov pomocou Grafany. Nainštalujte Grafana na server alebo stroj a nakonfigurujte ho na pripojenie k Prometheus ako zdroju údajov.
* Vytvorenie dashboardu: Po pripojení vytvorte v Grafane vlastné dashboardy na zobrazenie metrík výkonu siete. Použite intuitívne rozhranie Grafany na navrhovanie vizualizácií, ako sú čiarové grafy, stĺpcové grafy a tabuľky. Usporiadajte tieto vizualizácie do zmysluplných informačných panelov, ktoré poskytujú prehľad o rôznych aspektoch zdravia a výkonu siete.
* Výstrahy: Nakonfigurujte pravidlá výstrahy v Grafane, aby ste správcovia upozornili na akékoľvek abnormálne podmienky alebo odchýlky vo výkone. Využite integráciu správcu výstrah Prometheus na odosielanie upozornení prostredníctvom e-mailu, Slack alebo iných oznamovacích kanálov.
  1. Výhody integrácie:
* Monitorovanie v reálnom čase: Získajte prehľad o metrikách výkonu siete v reálnom čase, čo umožňuje proaktívne monitorovanie a rýchlu reakciu na problémy.
* Škálovateľnosť: Jednoducho prispôsobte monitorovací systém tak, aby vyhovoval ďalším zariadeniam a rozširujúcim sa požiadavkám na monitorovanie.
* Prispôsobenie: Prispôsobte ovládacie panely Grafana tak, aby vyhovovali špecifickým potrebám monitorovania a poskytovali prehľadné informácie na prvý pohľad.
* Historická analýza: Analyzujte historické trendy údajov s cieľom identifikovať vzory a efektívne optimalizovať sieťové zdroje.



Obr. 2 Grafická ukážka prepojenia

1. Záver

Ako autor tohto projektu vnímam integráciu SNMP Exporter, Prometheus a Grafana pre monitorovanie siete ako významný míľnik v modernizácii a optimalizácii postupov správy siete. V priebehu tohto projektu bolo čoraz evidentnejšie, že spolupráca týchto troch komponentov ponúka komplexné riešenie problémov, ktorým čelia správcovia sietí v dnešnom dynamickom a komplexnom prostredí.

Cesta začala uvedomením si potreby viditeľnosti metrík výkonu siete v reálnom čase. Tradičným monitorovacím prístupom často chýbala agilnosť a škálovateľnosť potrebná na udržanie kroku s vyvíjajúcou sa sieťovou infraštruktúrou. Vďaka integrácii SNMP Exporter, Prometheus a Grafana sa však objavila nová paradigma, ktorá sa vyznačuje proaktívnym monitorovaním, rýchlym riešením problémov a rozhodovaním na základe údajov.

Z praktického hľadiska proces implementácie odhalil prirodzenú synergiu medzi týmito komponentmi. Nastavenie nástroja SNMP Exporter poskytlo bezproblémové rozhranie na prístup k údajom o výkone zo zariadení s podporou SNMP, zatiaľ čo Prometheus slúžil ako centrálne úložisko na ukladanie a dopytovanie týchto údajov. Grafana so svojimi intuitívnymi možnosťami vizualizácie premenila nespracované metriky na použiteľné prehľady, čím umožnila správcom robiť informované rozhodnutia a efektívne optimalizovať sieťové zdroje.

Zoznam použitej literatúry

1. Prometheus: Prometheus docs. 2014. Aktualizovane 2024 [cit 2024-04-26]. Dostupné na internete: <<https://prometheus.io/docs/introduction/overview/>>
2. Prometheus: Prometheus github. 2014. Aktualizovane 26.04.2024 [cit 2024-04-26]. Dostupné na internete: <<https://github.com/prometheus/prometheus>>
3. James Turnbull: Monitoring with Prometheus. 2018. s 290-31, ISBN 0988820285, 9780988820289
4. Ubizen AETHIS: Security in SNMPv3 versus SNMPv1 or v2c. 2002. WayBack Machine cit 2013-04-29. Dostupné na internete: <<https://web.archive.org/web/20130429201847/http://www.aethis.com/solutions/snmp_research/snmpv3_vs_wp.pdf>>
5. Grafana: Grafana docs. 2014. Aktualizovane 2024 [cit 2024-04-26]. Dostupné na internete: <<https://grafana.com/docs/>>
6. Grafana: Grafana github. 2014. Aktualizovane 2024 [cit 2024-04-26]. Dostupné na internete: <<https://github.com/grafana/grafana>>
7. Bizety: Open Source Monitoring Stack: Prometheus and Grafana. 2019. Dostupné na internete: <<https://www.bizety.com/2019/01/25/open-source-monitoring-stack-prometheus-and-grafana/>>
8. Kolektív autorov: SNMP\_Exporter. 2015. Aktualizovane 2024 [cit 2024-04-26]. Dostupné na internete: <<https://github.com/prometheus/snmp_exporter>>
9. KC Kecheng: Performance Monitoring with Prometheus and Grafana. 2020. Dostupné na internete: <<https://performance-monitoring-with-prometheus.readthedocs.io/_/downloads/en/stable/pdf/>>