PROJEKT

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

Previazané s balíkom KPB1 – Návrh virt. riešenia

Previazané s výstupom V1 výsledok analýzy dostupných riešení

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1 LOGOVANIE A MONITOROVANIE V CLOUD PROSTREDÍ

Logovanie a monitorovanie je neoddeliteľnou súčasťou správy a udržiavania cloudových prostredí. Tieto procesy sú kritické pre zabezpečenie vysokého výkonu, dostupnosti a bezpečnosti cloudových služieb.

Logovanie je proces zaznamenávania udalostí, operácií a chýb, ktoré sa vyskytujú v systéme. V cloudovom prostredí, kde služby bežia na distribuovaných systémoch, poskytuje logovanie dôležité informácie pre analýzu a diagnostiku problémov. Umožňuje administrátorom a vývojárom sledovať detailné operácie celého systému, identifikovať a rýchlo riešiť vzniknuté problémy.

Monitorovanie je proces kontinuálneho zbierania, analýzy a vizualizácie dát o výkone a dostupnosti cloudových služieb. Umožňuje získať prehľad o stave infraštruktúry, aplikácií a služieb v reálnom čase. To zahŕňa sledovanie zdrojov ako CPU, pamäť, sieťové aktivity a využívanie úložiska, ako aj špecifické metriky aplikácií a služieb.

Kľúčové oblasti dôležitosti logovania a monitorovania:

- Bezpečnosť: Identifikácia bezpečnostných hrozieb a slabých miest, prostredníctvom analýzy logov a monitorovacích dát. V logoch sú uchovávané informácie o všetkých vykonaných operáciách a používateľov, pre ktorých boli vykonané
- Výkon: Optimalizácia využitia zdrojov a riešenie problémov s výkonom pred tým, než ovplyvnia koncových používateľov. Monitorovaním systémových metrík ako využitie CPU, pamäte, disku a ďalších, vieme v prípade ich nedostatku alebo nadmerného používania včasne reagovať.
- Dostupnosť: Rýchla diagnostika a náprava výpadkov alebo zlyhaní služieb. Zaznamenané a uložené logy tvoria informácie o celom systéme a bez prístupu k nim je až nemožné zistiť čo sa so systémom deje/dialo na vykonanie správnej diagnostiky.
- Súlad s právnymi normami: Dodržiavanie právnych a regulačných požiadaviek týkajúcich sa zaznamenávania a uchovávania dát, z hľadiska tzv. právnej nepriestrelnosti. Je potrebne udržiavať údaje o činnosti prístupoch ktoré boli uskutočnené v systéme, v prípade spätného získavania informácií.

1.1 Pokročilé logovacie stratégie

Zahŕňajú agregáciu, koreláciu a analýzu logov z rôznych zdrojov a služieb. Vyspelé techniky ako centralizované logovacie platformy a logovací agenti umožňujú efektívne spracovanie a skladovanie zalogovaných dát. Jedným zo známych riešení je použitie ELK Stack (Elasticsearch pre vyhľadávanie a analýzu, Logstash pre agregáciu a transformáciu logov a Kibana pre vizualizáciu) alebo podobných riešení, ktoré umožňujú hlbokú analýzu a získavanie užitočných informácií z obrovských objemov logovaných dát. [6]

1.1.1 Pokročilé monitorovacie techniky

Využívajú kombináciu pasívneho a aktívneho monitorovania, pre získavanie komplexného prehľadu o stave infraštruktúry a aplikácií. Pasívne monitorovanie kontinuálne sleduje systémové metriky a výkonnostné ukazovatele, zatiaľ čo aktívne monitorovanie zahŕňa generovanie a spracovanie testovacích transakcií na meranie reakčných časov a dostupnosti služieb. Riešenia ako Prometheus, kombinované s Grafanou pre vizualizáciu, poskytujú nástroje pre zber, ukladanie a analýzu metrík v reálnom čase. [6]

1.1.2 Analýza a korelácia udalostí (Event Correlation and Analysis, ECA)

Predstavuje vyspelú techniku v rámci monitorovania, ktorá umožňuje identifikáciu a automatické riešenie známych problémov prostredníctvom korelácie rôznych udalostí a metrík. Táto metóda zvyšuje efektivitu správy systému tým, že minimalizuje falošné poplachy (false positives) a umožňuje rýchlejšiu diagnostiku a riešenie problémov. Ako príklad sa dá pozrieť na sledovanie metrík a logov. Ak sledujeme náš systém s enormným využitím zdrojov a logy vykazujú veľký počet zamietnutých pokusov o prístup do systému, môžeme predpokladať, že sa jedná o nejaký útok a na koreláciu týchto dvoch eventov vieme konkrétnejšie a automaticky reagovať. [7]

1.1.3 Bezpečnostné aspekty logovania a monitorovania

Týkajú sa nielen zachytávania a analýzy bezpečnostných incidentov, ale aj zabezpečenia samotných logov a monitorovacích dát. Implementácia silných autentifikačných a autorizačných mechanizmov, šifrovanie dát pri prenose a ukladaní, a pravidelné auditovanie prístupu a aktivity sú nevyhnutné pre ochranu citlivých dát a zabezpečenie súladu s regulačnými požiadavkami.

1.1.4 Automatizácia

Hrá kritickú úlohu v logovaní a monitorovaní tým, že umožňuje automatické nasadenie monitorovacích agentov, konfiguráciu prahových hodnôt a upozornení alebo vykonávanie preddefinovaných akcií na základe detekcie špecifických udalostí alebo metrík. Použitie IaC (Infrastructure as Code), konfiguračných a manažovacích nástrojov ako Ansible, Puppet, bash atď., umožňuje konzistentné a opakovateľné nasadenie a konfiguráciu logovacích a monitorovacích služieb naprieč cloudovou infraštruktúrou.

Pre účinné logovanie a monitorovanie je dôležité nielen vybrať správne nástroje, ale aj definovať politiky a postupy pre spracovanie logov, nastavenie prahových hodnôt pre upozornenia a automatizáciu reakcií na identifikované problémy. Taktiež potreba vytvorenia alarmovacích systémov pre automatické oznamovanie/reagovanie podľa vopred predefinovaných pravidiel.

1.1.5 Alarmovanie

Pri zbere všetkých metrík a logov zo všetkých modulov, aj keď sa všetko nachádza v jednom centralizovanom systéme, stále je veľmi ťažké mať prehľad o všetkých uložených informáciách, metrikách a logoch. Existujú alarmovacie systémy ako Prometheus Alerts alebo Grafana Alerts. Vďaka týmto systémom je možné si nastaviť pravidlá, ktoré budú sledované za nás a v prípade ich prekročenia je možné nastavenie zasielania notifikácií do platforiem ako Microsoft Teams alebo Discord. Notifikácie je možné zaslať do ľubovoľnej platformy, ktorá podporuje web hooks. Pri Grafana Alerts je možné si vytvoriť pravidlo. Pravidlu sa nastaví Querry, ktorá bude získavať aktuálne údaje z logov alebo metrík. Tie sú porovnávane s nastavenou hranicou. Ak sa táto hranica prekročí, tak alert prejde do iného stavu. Stavy ktoré sa tu nachádzajú sú:

- Normal – normálny stav sledovanej metriky, resp. hodnoty z Querry
- Pending – Sledovaná hodnota minimálne jeden raz prekročila nastavenú hraničnú hodnotu za určitý čas
- Firing – Sledovaná hodnota neklesla pod hraničnú v sledovaných intervaloch niekoľko krát za sebou

Alarm ktorý sa nachádza v stave Firing tak prechádza do Notifikačnej politiky, v ktorej sú nastavené pravidlá ohľadom zasielania Notifikácií. Tieto Alarmovacie systémy sú nevyhnutné pre včasne reagovanie, zjednodušenie a prehľad o celom monitorovanom systéme bez toho aby bolo potrebné pozerať do tohoto monitorovacieho a logovacieho systému.

2 Logovanie a monitorovanie OpenStack

OpenStack, ako komplexná open-source platforma CC, ponúka robustné možnosti pre správu a automatizáciu rozsiahlych virtuálnych infraštruktúr. Efektívne logovanie a monitorovanie sú kritické pre udržanie vysokého výkonu, bezpečnosti a dostupnosti v OpenStack Cloudoch. Tieto mechanizmy umožňujú operátorom identifikovať, diagnostikovať a riešiť problémy a zároveň optimalizovať využitie zdrojov.

2.1 Logovanie v OpenStack

Centralizované logovanie je základnou požiadavkou pre efektívnu správu OpenStack nasadení. Z dôvodu rozptýlenosti komponentov OpenStacku po rôznych uzloch je nevyhnutné zaznamenávať logy do centralizovaného úložiska, ktoré umožňuje agregáciu, vyhľadávanie a analýzu logov. Projekty ako Elasticsearch, Logstash a Kibana (ELK) alebo Graylog sú často využívané pre ich flexibilné možnosti spracovania a vizualizácie logov.

Logovacie úrovne v OpenStack sa dajú nastaviť pre rôzne komponenty, čo umožňuje detailné sledovanie činností systému alebo obmedzenie logovania na kritické udalosti pre zníženie objemu dát. Táto flexibilita je dôležitá pre efektívnu diagnostiku a minimalizáciu vplyvu na výkon.

2.2 Monitorovanie v OpenStack

Monitorovanie výkonu a dostupnosti komponentov OpenStack je zabezpečené prostredníctvom rôznych nástrojov a techník. Projekty ako Ceilometer a Monasca ponúkajú rozsiahle možnosti pre zber metrík, monitorovanie zdrojov a generovanie upozornení. Tieto nástroje získavajú údaje z rôznych častí OpenStacku a podporujú automatizovanú reakciu na udalosti v systéme.

Ceilometer slúži na zber údajov o využití zdrojov a metrík z OpenStack inštancií a služieb pre účely fakturácie používateľom, benchmarkingu a monitorovania, dokáže zaznamenávať informácie o využití výpočtových zdrojov, úložiska a sietí, čím poskytuje základ pre analýzu výkonnosti a optimalizáciu prostriedkov.

Monasca(Monitoring-as-a-service) je vysoko škálovateľná Multi-tenant monitorovacia platforma pre OpenStack, ktorá poskytuje funkcie pre zber, ukladanie, vyhľadávanie a vizualizáciu metrík a logov. Monasca podporuje alarmovanie a notifikovanie, umožňuje rýchlu identifikáciu a riešenie problémov.

Logovanie a monitorovanie sú neoddeliteľnou súčasťou správy a udržiavania OpenStack prostredí. Implementácia pokročilých logovacích a monitorovacích stratégií zvyšuje transparentnosť, umožňuje rýchlu identifikáciu a riešenie problémov, zlepšuje bezpečnosť a optimalizuje využitie zdrojov. Vyžaduje si to však starostlivý výber nástrojov, konfiguráciu a neustále sledovanie, aby boli zabezpečené vysoké štandardy dostupnosti, výkonu a bezpečnosti.

3 Openstack Charms, z pohľadu monitorovania

OpenStack Charms umožňuje integráciu s populárnymi monitorovacími a logovacími platformami ako sú Nagios, Zabbix a Prometheus alebo ELK Stack. Pre túto integrácia sú vyvinuté Juju charms, ktoré automatizujú celé nasadenie a aj konfiguráciu monitorovacích agentov na OpenStack moduloch, ako aj zber a exportovanie metrík a logov do centrálneho monitorovacieho systému. Pri nasadení nového uzla alebo služby OpenStack prostredníctvom Charms, môžu byť súčasťou procesu automatizovane pridaný aj monitorovací agenti a príslušné konfiguračné nastavenia. To znižuje potrebu manuálnych krokov, zjednodušuje udržiavanie chodu aplikácií a konzistentnosť monitorovania naprieč celou Cloudovou infraštruktúrou. Automatizovaný prístup patrí medzi najdôležitejšie vlastnosti pri nasadzovaní a udržiavaní dnešných služieb.

V tomto nasadení je treba myslieť na rozptýlenosť modulov v kontajnerizovanom prostredí, kde niektoré z modulov sú nasadené v kontajneroch pre určitú konzistentnosť, izolovanosť balíčkov a nástrojov ktoré používajú. Moduly ako Nova sú nasadené priamo na fyzických uzloch pre priamy prístupu a prideľovanie zdrojov virtuálnym zariadeniam. Je potrebné brať ohľad na umiestnenia, či už logovacích výstupov, súborov alebo pri zbieraním metrík z konkrétnych lxc kontajnerov a uzlov. Juju charms majú ponúkať lepší a jednoduchší prístup pri nasadení, pri manažovaní celého životného cyklu, ale aj pri oprave vzniknutých chýb, pri reakcií na vzniknuté eventy, škálovaní atď. Juju charms sú tvorené z väčšej časti Python kódom alebo bash skriptami. Celé nasadenie musí byť preddefinované a naprogramované, každý jeden hook alebo vzťah medzi jednotlivým komponentami musí byť tak isto implementovaný v Python charms. Vzniká tu potreba implementácie celej funkcionality, čo znamená, že ak chcem aplikáciu nasadiť a manažovať pomocou charms, musím jej konfiguráciu definovať v kóde. Ak táto aplikácia vyžaduje pripojenie na databázu, musí to byť naprogramované. To isté platí aj pri monitorovaní. Ak nám túto funkcionalitu autori charms nevytvorili – nevieme ju vykonať. Canonical má tiež jedno monitorovacie riešenie s názvom COS, ktoré si rozoberieme neskôr.

4 Zhrnutie aktuálneho stavu

Informácie o logoch sú dostupné iba na konkrétnych strojoch, na ktorých dané OpenStack moduly bežia a zaznamenávajú si logy. Tieto nie sú žiadnym spôsobom zbierané, udržiavané, zálohované ani analyzované. Pre metriky platí to isté, avšak niektoré základné informácie o obsadenosti zdrojov sú dostupné v Horizon dashboard-e pre OpenStack. Toto riešenie nie je dostačujúce, slúži iba pre informačné účely. Pre zistenie aktuálnych a reálnych hodnôt metrík systémov existuje jediný spôsob a to prístup na výpočtové uzly a použitie linuxových balíčkov ako TOP a jemu podobné. Tento stav je zo všetkých spomenutých hľadísk neprístupný. Je potrebné analyzovať a vybudovať centralizovaný prístup ku všetkým týmto logom a metrikám.