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
V3 – Popis vybraného riešenia spĺňajúceho stanovené kritéria

typ – dokumentácia

Analýza II. - Graylog

OBSAH

1 Graylog 4
1.1 Produkty Graylog 4
1.2 Hlavné funkcie 5
2 Inštalačné požiadavky 6
2.1 Graylog stack 6
2.1.1 Porty 6
2.1.2 Odporúčané systémové požiadavky 6
2.1.3 Shard 7
2.1.4 Kompatibilita 7
3 Popis funkcií 8
3.1 LOGOVANIE DÁT 8
3.1.1 Logovacie vstupy 8
3.2 Data Routing 8
3.2.1 Streams 8
3.2.2 Pipelines 8
3.2.3 Destinácie 8
3.3 Vyhľadávanie dát 9
3.4 Vizualizácia dát 9
3.5 Udalosti a upozornenia 9
3.5.1 Event 9
3.5.2 Alert 9
Zdroje 9

1 GRAYLOG

Graylog je výkonné riešenie pre správu bezpečnostných informácií a udalostí (SIEM), ktoré ponúka robustnú platformu na analýzu logov, zjednodušujúcu zber, vyhľadávanie, analýzu a upozornenia na všetky typy dát generovaných strojmi. Je špecificky navrhnutý na zachytávanie dát z rôznych zdrojov, čo umožňuje efektívne centralizovať, zabezpečovať a monitorovať logy. Graylog dokáže vykonávať širokú škálu kyberbezpečnostných funkcií, ako napríklad:

- Agregácia dát
- Analýza bezpečnostných dát (reporty a dashboardy)
- Monitorovanie bezpečnostných udalostí
- Forenzná analýza
- Detekcia incidentov a reakcia na ne
- Konzola pre odozvu na udalosti v reálnom čase alebo upozornenia
- Threat intelligence (inteligencia o hrozbách)
- Analýza správania používateľov a entít (UEBA)

1.1 PRODUKTY GRAYLOG

Graylog má na výber niekoľko verzií z ktorých možno vybrať. Každá verzia ponúka iné riešenia pre správu logov. Pre používanie však vyžadujú platenú licenciu, ponúka však aj open-source verziu ktorá je voľne dostupná.

Verzie Graylog:

1. **Graylog Open**: Bezplatná open-source verzia poskytujúca základnú správu logov s možnosťami zhromažďovania, obohacovania a analýzy dát.
2. **Graylog Enterprise**: Obsahuje všetky možnosti Graylog Open, pričom pridáva pokročilé funkcie, ako sú archivácia logov, audit používateľov, notifikácie na báze skriptov, plánované reporty a technickú podporu. Tento balík je určený pre organizácie s komplexnými IT infraštruktúrami.
3. **Graylog Security**: Doplnenie k Enterprise verzii zamerané na kybernetickú bezpečnosť. Umožňuje detekciu, vyšetrovanie a reakciu na bezpečnostné incidenty s funkcionalitou na hrozbové spravodajstvo a monitoring správania používateľov.
4. **Graylog Cloud**: Kombinuje výhody Graylog Enterprise a Security s flexibilitou cloudového prostredia. Je to plne spravovaná služba, ktorá umožňuje rýchle nasadenie, škálovanie a aktualizácie bez potreby vlastnej infraštruktúry.
5. **Graylog API Security**: Produkt určený na ochranu API, poskytuje detailný prehľad o činnosti API a identifikuje prípadné zneužitia.
6. **Graylog Illuminate**: Doplnkový balík pre Enterprise a Security verzie, ktorý poskytuje predpripravený obsah (pipelines, pravidlá, lookup tabuľky) na spracovanie logov pre konkrétne operácie.

1.2 HLAVNÉ FUNKCIE

Hlavné funkcie ktoré ponúka riešenie Graylog:

Streams (Prúdy): Slúžia ako tagy pre prichádzajúce správy a kategorizujú ich v reálnom čase. Pomocou pravidiel možno určiť do ktorého prúdu bude správa smerovať.

Vyhľadávanie: Stránka Graylog Search umožňuje priame vyhľadávanie v logoch pomocou jednoduchej syntaxe podobnej Lucene. Časové intervaly môžu byť relatívne alebo absolútne a výsledky sa dajú uložiť alebo zobraziť ako agregácie, ktoré je možné pridať na dashboardy.

Dashboardy: obsahujú vizualizácie alebo zhrnutia informácií ktoré sa nachádzajú v logoch. Dashboard je možné prispôsobiť widgetmi, ktoré vizualizujú dáta (počty, priemery, grafy, mapy), a sú dostupné ovládanie prístupu na základe rolí.

Upozornenia (Alerts): Vytvárajú sa pomocou pravidiel udalostí. Po splnení určitej podmienky sa spustí udalosť, ktorá môže aktivovať upozornenie.

Indexy: Slúžia ako základné úložné jednotky dát, pričom indexy umožňujú nastavenie retencie, shardingu a replikácie pre konkrétne dáta, s možnosťou prispôsobiť ich uchovávanie a rotáciu.

Graylog Sidecar: Tento agent spravuje logovacích klientov, ktorí zbierajú logy z OS serverov a posielajú ich do Graylogu.

Procesné pipeline: Umožňujú aplikovať pravidlá na konkrétne typy udalostí, pričom správy môžu byť podľa potrieb upravené, obohatené alebo zablokované, čo optimalizuje ich spracovanie cez Graylog.

2 INŠTALAČNÉ POŽIADAVKY

2.1 GRAYLOG STACK

Graylog architektúra je zložená z troch komponentov nazývaných aj Graylog stack:

1. Graylog
2. Data node (OpenSearch)
3. MongoDB

Graylog samotný je webové rozhranie ktoré slúži ako kontrolne centrum pre manažment logovacích dát. Užívateľom dovoľuje efektívne filtrovať a analyzovať logy zozbierané z rôznych zdrojov.

Data Node je komponent architektúry Graylog ktorý je zodpovedný za manažovanie OpenSearch. Táto funkcia dovoľuje Graylogu manažovať backend pre vyhľadávanie aby nebolo potrebné inštalovať a manažovať OpenSearch separátne. Zlepšuje bezpečnosť dátovej vrstvy implementovaním certifikátov. Zabezpečuje aj korektnú verziu OpenSearch a jeho rozšírení.

MongoDB je NoSQL databáza zodpovedná za ukladanie metadát a configuračných dát pre Graylog. Slúži aj na ukladanie dát pre OpenSearch nodes čo zabezpečuje redundačnosť a prístup dát. MongoDB je tiež škálovateľná čo ju robí ideálnou pre veľké množstvo dát. Na svoj beh potrebuje iba malé množstvo systémových zdrojov a ukladacieho priestoru.

2.1.1 Porty

Pre plynulé fungovanie potrebuje Graylog prístup k nasledjúcim portom:

- :9000 – Na tomto porte pracuje Graylog API, ktorý musí byť dostupný pre všetky Graylog uzly
- :443 – HTTPS port
- :9515 – ChromeDriver pre generovanie reportov
- :27017 – MongoDB
- :514 – Syslog vstup
- :1514 – Alternatívny syslog port
- :4739 – NetFlow vstup
- :5044 – Beats vstup
- :5555 – Graylog Extended Log Format (GELF)

2.1.2 Odporúčané systémové požiadavky

Systémové požiadavky sa môžu líšiť podľa množstva očakávaných dát. Odporúčané požiadavky pre spracovanie 1-10 GB dát za deň sú:

- 8 Jadrový CPU
- 16 GB RAM

Pre dátový uzol je odporúčané:

- 8 Jadrový CPU
- 24 GB RAM

2.1.3 Shard

Shard je je v podstate časť dát v databáze alebo vyhľadávacom nástroji. Shards sú kľúčové pre výkon a škálovanie Graylog systému a distribujú dáta naprieč viacerými dátovými uzlami.

2.1.4 Kompatibilita

Graylog je možné nainštalovať takmer na akejkoľvek distribúcií Linux.

Pri inštalovaní Graylog je potrebné dodržať kompatibilitu s ostatným softvérom. Verzia Graylog 6.1 má nasledovné požiadavky:

- Minimálna verzia MongoDB: 5.0.7
- Maximálna verzia MongoDB: 7.x
- Minimálna verzia OpenSearch: 1.1.x
- Maximálna verzia OpenSearch: 2.15.x

3 POPIS FUNKCIÍ

3.1 LOGOVANIE DÁT

3.1.1 Logovacie vstupy

Logovacie vstupy slúžia na akceptovanie logovacích správ v Graylogu. Niektoré základné typy správ sú podporované Graylogom, iné je potrebné doinštalovať cez pluginy. Vstupy sú ďalej delené na listener a pull.

Listener vstupy počúvajú na porte pre danú aplikáciu a posielajú dáta do Greylogu.

Pull vstupy komunikujú s koncovými zariadeniami a vyberajú logy pomocou API alebo iných metód.

Medzi bežné vstupy patria:

- Ingest syslog
- Ingest journald
- Ingest Windows eventlog
- Ingest CEF
- Ingest Raw/Plaintext
- Ingest GELF
- Ingest from files
- Ingest JSON path from API
- Ingest Application Data

Pre bezpečný prenos dát je možné povoiť TSL šifrovanie pre jednotlivé vstupy

3.2 DATA ROUTING

Po prijatí logov Graylogom je ďalší krok filtrovať, upraviť a dalej posielať tieto logy do cieľových destinácií.

3.2.1 Streams

Po prijatí logov do Graylogu sa dajú logy priradiť ku konkrétnym streamom, čo sú špecifické procesy používané na filtrovanie a smerovanie logov cez Graylog a mimo neho. Streamom sa dajú priradiť pravidlá ktoré určujú, aké správy sú smerované do ktorého streamu.

3.2.2 Pipelines

Pomocou pipelines môžeme správy transformovať a upraviť po tom, čo sú poslané do streamu. V podstate je to sekvencia procesov, cez ktoré správa prechádza. Môžu to byť operácie ako filtrovanie, transformácie alebo preposielanie.

3.2.3 Destinácie

Po spracovaní sú dáta posielané na výstup do:

- Indexových setov (Index Sets) – uložný priestor pre logy, tie sú tu uložené podľa určitých vlastnosti alebo potrieb.
- Výstupov (Outputs) – posielanie dát do externých systémov alebo destinácií.

3.3 VYHĽADÁVANIE DÁT

Vyhľadávať dáta je možné vo webovom rozhraní Graylog. Vyhľadané dáta sú vizualizované cez rôzne widgets. Vyhľadané logy sa dajú uložiť a exportovať.

3.4 VIZUALIZÁCIA DÁT

Dáta sú vizualizované cez widgets. Pomocou widgets môžeme zobraziť dáta do rôznych perspektív. Dáta môžu byť zobrazené v grafe alebo tabuľke. Na vizualizáciu dát je možné použiť aggregation widgets alebo message table widgets.

Aggregation widgets sú dáta formované tak, aby jasne odpovedali na špecifickú otázku. Zobrazujú iba požadované polia, funkcie alebo metriky. Môžu to byť napríklad správy z určitej IP adresy z posledných dvoch dní.

Message table widgets zobrazujú správy a ich polia. Je to detailnejšie vyšetrenie jednotlivých správ.

3.5 UDALOSTI A UPOZORNENIA

3.5.1 Event

Event (udalosť) je zmena v prostredí ktorá je iná od očakávaného správania. Môže to byť napríklad zmena vo firewall pravidlách alebo neúspešný pokus o prihlásenie zo zablokovanej adresy. V Graylogu je možné nastaviť parametre pre udalosti a ak dáta spĺňajú parametre, graylog vyhodí alert (upozornenie).

3.5.2 Alert

Alert (upozornenie) je notifikácia ktorá sa dá vytvoriť pre event.

ZDROJE

https://go2docs.graylog.org/current/what_is_graylog/what_is_graylog.htm