Jak na log management

Lukáš Macura
CESNET

Obsah

- Proč?
- Principy
- Sběr
- Nástroje
- Bezpečnost
- Škálovatelnost
- Analýza a reakce na incidenty
- Nejlepší praktiky
- Závěr

Proč?

- Log management je vyžadován mnoha doporučeními
  - **ISO/IEC 27001 (Systémy řízení bezpečnosti informací)**
  - **ISO/IEC 20000 (Řízení IT služeb)**
  - **NIST SP 800-53 (Doporučení pro bezpečnostní kontroly)**
  - **COBIT (Control Objectives for Information and Related Technologies)**
  - **GDPR (Obecné nařízení o ochraně osobních údajů)**
  - **ITIL (IT Infrastructure Library)**
  - **NIS2 (Directive on Security of Network and Information Systems 2)**

Proč?

- Nemohu reagovat na incident, pokud o něm nevím

Proč?

- Musím být schopen zpětně dokázat, jak se událost stala

Proč?

- Je vždy výhodnější problémům předcházet
- Víte, kolik neúspěšných pokusů o přihlášení se děje na vašich serverech?

Principy

- Sběr
- Odkud sbírat logy?
- Znám všechny své systémy?
- Potřebuju asset management

Sběr

- Transport
- RFC 3164 - The BSD syslog Protocol
  - nestrukturované data (text)
- RFC 5424 - The Syslog Protocol
  - nestrukturované data (text)
- GELF
  - Data zabalená v JSON, mohou být více strukturovaná
- BEATS
  - Strukturovaná data
- SSL/TLS
- Autentizace zdroje
- Autentizace serveru

Sběr

- Neměnit po cestě transport syslog zprávy
- Některé agenty umí jen některý transport
- Oddělené cesty (například jiný port)
- Ideálně srovnat už u zdroje
- Používat stejnou template na všech agentech
- Používat jeden identifikátor hosta přes celou síť (FQDN)

Sběr

- Jak sbírat non-syslog soubory?
- rsyslog

```
module(load="imfile" PollingInterval="10" statefile.directory="/var/spool/rsyslog")
input(type="imfile"
      File="/var/log/apache2/access.log*"
      Tag="apache2_http_access"
      reopenOnTruncate="on"
      Severity="info"
      Facility="local6")
```

Sběr

- Jak sbírat non-syslog soubory?
- Syslog-ng

```
source s_nginx_a { file("/var/log/nginx/access.log" program-override("nginx_web_http_access")); };
source s_nginx_e { file("/var/log/nginx/error.log" program-override("nginx_web_http_error")); };
```

Nástroje - sběr

- syslog-ng
- rsyslog
- Beats
- Nxlog (Windows)

Nástroje - agregace

- Syslog-ng
- Rsyslog
- A jiné, komerční varianty
- grep jako nejmocnější nástroj

Nástroje - indexace

- Vyžaduje mnohem větší zdroje než agregace
- Bottleneck všech logovacích systémů
- Nesmíme přehltit
- Ale zároveň bychom o žádné data neměli přijít
- ELK
- Graylog
- A komerční nástroje…
- Indexované data jsou mnohem mocnější než grep
- Ale retence výrazně menší

Nástroje - analýza

- Nejsložitější část
- Vyžaduje zdroje
- Vyžaduje patterny
- Vyžaduje pozornost a nastavení
- Graylog
- ELK
- A další, komerční varianty

Bezpečnost

- Používat ideálně TLS
- Nevěřit položkám v syslog zprávě (jako hostname)
- Jediné, co je důvěryhodné, je zdrojové IP a certifikát
- Pohlídat, kdo má přístup k logům
- Mít logy na více místech
- Mít dostatek disku pro retenci
- Monitorovat chod celého systému

Bezpečnost

- Mnoho vendorů se snaží ulehčit práci
- Agenti běží jako root a distribuují config klientům
- Pozor na to. Ideální napsat si svůj Ansible script

Škálovatelnost

- Více centrálních serverů pro indexing a analýzu
- Ale i to má strop (hlavně cena)
- Pokud možno použít agenty pro “hrubou práci” (BEATS)
- Na centrálním místě indexing a analýza

Analýza a reakce na incidenty

- Komerční systémy mohou automaticky obsahovat
- U opensource “stará dobrá ruční práce”
- Ale pozor na detaily. Mnohdy sice vendor tvrdí, že něco umí analyzovat, ale situace může být jiná
- Mravenčí práce, pokud se to má dělat inhouse. Je mnoho druhů syslog zpráv a aplikací
- A k tomu mnohdy ještě lokální aplikace, které jinak než ručně nejdou

Nejlepší praktiky

- Začněte logovat
- Začněte logy agregovat (centrální server)
- Udělejte analýzu, jestli opravdu všechny assety logují
- Pohlídejte si backup a správnou retenci
- Začněte indexovat
- Začněte analyzovat
- Udělejte jednoduchý návod, jak nastavit agenta nebo Ansible

Závěr

- Dotazy