cesnet

JAK NA CENTRÁLNÍ LOG MANAGEMENT

Lukáš Macura, CESNET

Leden 2025, CSNOG

cesnet

OBSAH

- Kdo/co/odkud/proč by měl logovat?
- Jak logovat?
- Čím logovat?
- Čím analyzovat?
- Závěr

PROČ?

- 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)

KDO?

- Všichni správci systémů
- Neexistuje omluva nebo výmluva
- Zodpovědnost
  - Správce systému
    - Formát a transport logů
    - Aktuálnost logů
  - Manažer
    - Pokrytí všech systémů
  - Vývojáři aplikací
    - Data

- Všechno
- Pohlídat aplikační data, log by neměl obsahovat citlivá data
- Většina běžných aplikací loguje správně, i s debugem
- Pozor na vlastní aplikace a data, které logují
- Špatně: Successful login, user=root, password=123456
- GDPR vs log retention

ODKUD?

- **Ze všech systémů**
- **Obecně:**
  - Co je produkční
  - Co obsahuje produkční data
  - Co je dostupné z Internetu
  - Co má přístup na Internet
  - Všechny síťové zařízení
  - Ideálně logovat alespoň všechny dropped packety

ČÍM?

- Rsyslog
- Syslog-ng
- Nxlog (Windows)
- BEATS

Syslog (RFC5424)

- **Nemixovat log transport (RFC5424 vs RFC3164) na jednom portu**
- **Ideálně: TLS transport s autentizací certifikátem, jinak alespoň TCP**
- **Primární důvěra v source IP**
- **Sekundární v CN certifikátu**
- **Terciální v HOST makro ve zprávě (nedůvěryhodné)**
- **+ Grep compatible (rychlost, jednoduchá archivace a retence)**
- **- Složitější analýza (parsování) na straně serveru**
- /var/log/clm/<trusted-ip>/<host>/<host>_<isodate>_<trusted-ip>_<trusted-cn>_<transport>.log

GELF (pro Windows a NXLog)

- **JSON formát**
- **- Nevhodné pro přímé ukládání do streamů na disk**
- /var/log/clm/<trusted-ip>/<host>/<host>_<isodate>_<trusted-ip>_<trusted-cn>_<transport>.json

BEATS

- Pokud je potřeba dalších analýz
- Pro Graylog a další
- - Nutná orchestrace na agentech
- - Nevhodné pro přímé ukládání do streamů na disk
- + Offload analýzy na agenta

- Fail2ban, Crowdsec: Pro centrální reakci na incidenty
- Zabbix: Pro monitoring logů, případnou reakci na vybrané logy

Graylog

- Pro analýzu a korelaci logů
- Možno použít i jiné nástroje (Wazuh, ELK, ...)
- Opensource řešení obecně náročnější, ruční definice pravidel
- - Některé detekce nefungují při syslog transportu
- - Velmi náročné na zdroje
- - Malá retence

cesnet

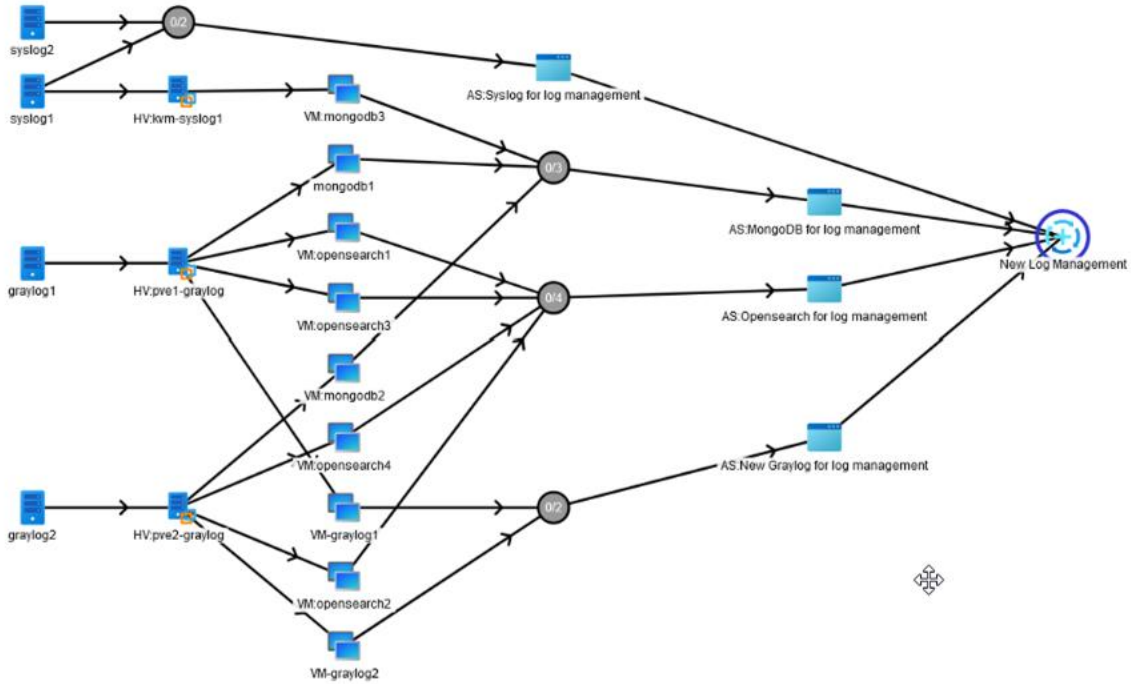
ZÁVĚR

- Logujte
- Dokud nelogujete, nevidíte
- Pokud nelogujete centrálně, nemůžete korelovat
- Použijte alespoň základní, automatickou analytiku
- Reagujte a upravujte analytiku dle incidentů

cesnet

~~ZÁVĚR~~ POKRAČOVÁNÍ

- Dotazy?
- Odpovědi?



cesnet

DĚKUJI ZA POZORNOST

LUKÁŠ MACURA
LOG MANAGEMENT TÝM