

Logování a monitoring produkčních aplikací

Tomáš Jecha

Microsoft Most Valuable Professional (MVP)

Vývojář, softwarový architekt, lektor

tomas@jecha.net

Logy emailem?

Rychlá notifikace pro menší projekty

Špatné vyhledávání a agregace

Rezignace příjemců – ztráta hlavní výhody

Větší množství zpráv = nepoužitelné

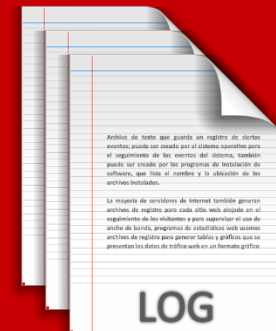
▷ **Inbox** 10986

Drafts [1]

Sent Items

Logy do textového souboru?

Ověřené a jednoduché
Vhodné pro dodatečnou analýzu
Bez další infrastruktury není vhodný pro live monitoring
Decentralizovaný přístup



Logy do aplikační databáze?

Centralizovaný přístup

Dotazování a agregace

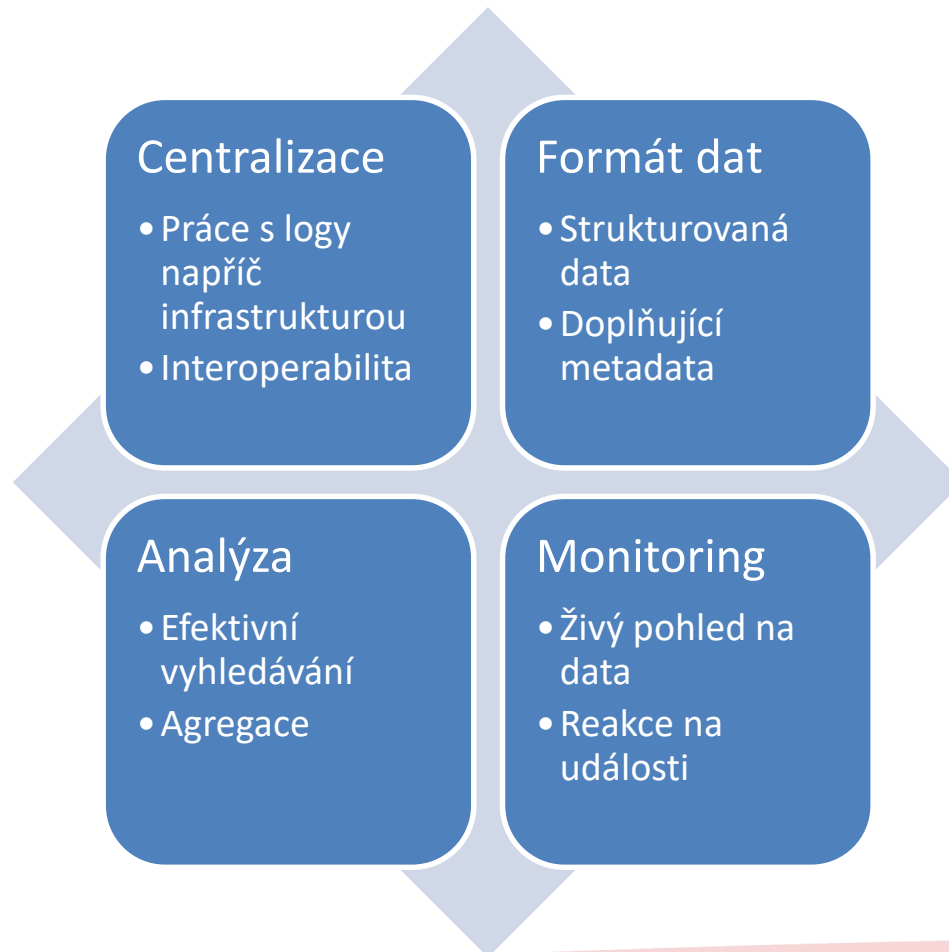
Živý pohled

Jaká databáze?

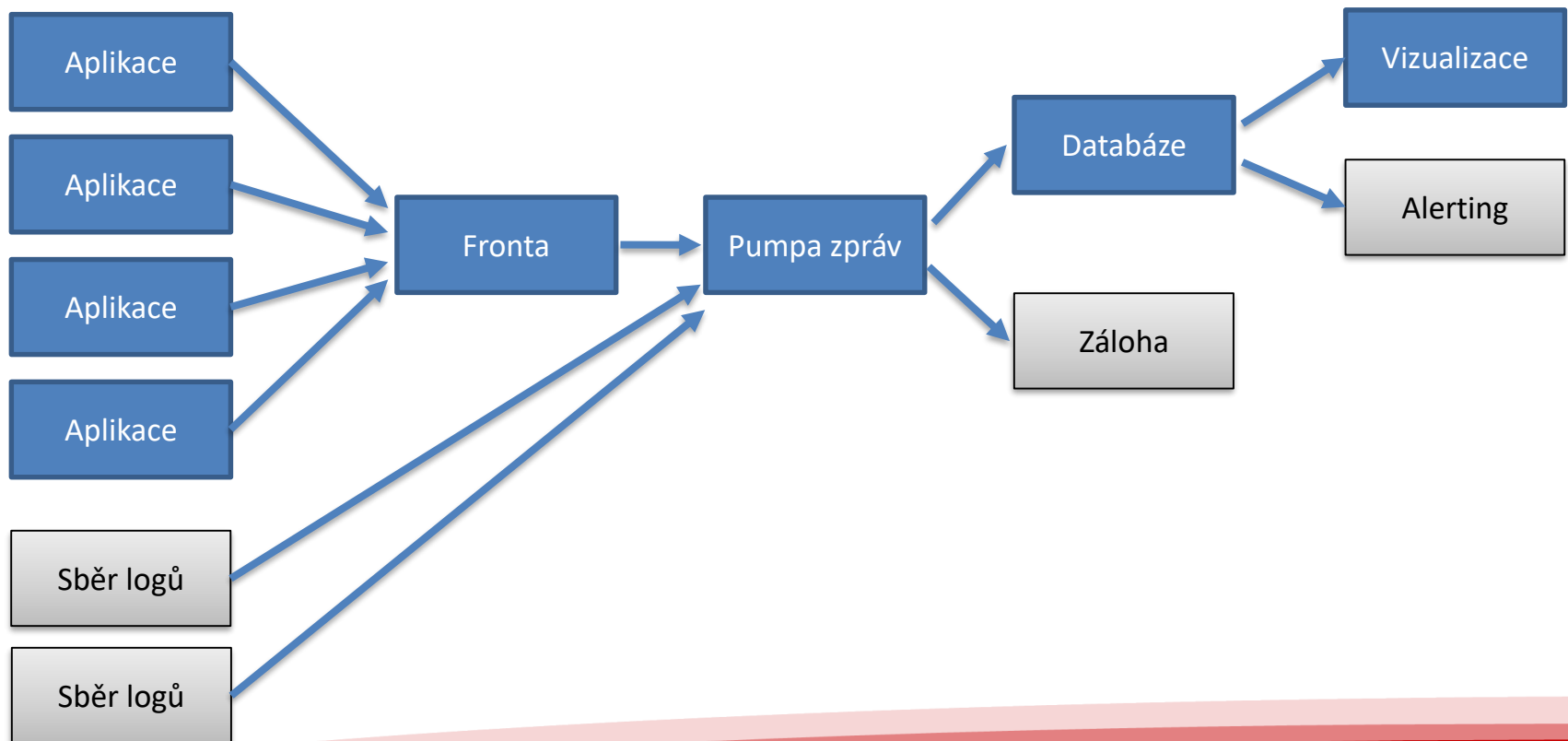
(relační vs dokumentová, cena, rychlost, server)



Požadavky na logování



High level architecture



Použité technologie

- Elastic Search – full text document DB
- Kibana – vizualizace dat z ES
- Logstash – pumpa zpráv
- RabbitMQ – fronta (buffer, routing a HA)
- Serilog – logovací framework pro .NET
- *Beats – sběr logů*

Instalace RabbitMQ a napojení aplikací



demo

Instalace Elastic Search + Kibana + LogStash



Analýza logů

- Vyhledávání
- Filtrování
- Seskupování
- Časový histogram

Analýza logů



demo

Tomáš Jecha

tomas@jecha.net