Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Monitoring & logging bij DUO

Frits Bouma (frits.bouma@duo.nl)
Architect bij CIO-Office DUO

Gegevens Digitale Overheid | 18 oktober 2017

Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Monitoring & logging bij DUO

Korte presentatie:

- Waarom monitoring & logging?
- Veranderende mogelijkheden
- Veranderende eisen
- Veranderende wensen
- Keuzes
- Toekomst
- Tijd voor vragen

Gegevens Digitale Overheid | 18 oktober 2017

Waarom monitoring?

- Verstoring van systemen (IT, processen, omgeving) opmerken
- Signaleren van poging tot inbraak
- Biedt mogelijkheid om in te grijpen / bij te sturen

Waarom logging?

- Monitoring levert slechts een momentopname
- Voor rapportage en verantwoording moeten monitoringgegevens bewaard blijven
- Historische gegevens leveren een baseline voor “normaal” gedrag van systemen
  - Nodig om afwijkingen te kunnen constateren
  - Nodig om effecten van bepaalde keuzes te kunnen meten (leren van ervaringen)
  - Nodig om effectiviteit van genomen maatregelen te toetsen
- Prognoses kunnen maken (trendanalyses, extrapolatie)
- Biedt geheugen dat foutherstelling (rollback) mogelijk maakt
- Onweerlegbaarheid aantonen (auditeerbaarheid)

Verandering maatschappij

Begin jaren 80:

- Single channel: post + data entry afdeling
- Verwerking ‘s nachts met batch-systemen
- Beschikkingen en informatie per uitgaande post
- Uitwisseling met ketenpartners op tape per koerier
- LAN -> gesloten

Heden:

- Multi channel: interactief portaal, app, webservices (M2M-verkeer), (digitale) post;
- 24/7 real-time verwerking;
- WAN -> open

Historie bij DUO: platformen

Begin jaren 80 klassiek ontwerp & realisatie informatiesystemen:

- Mutatielogging bij data entry was vanzelfsprekend onderdeel van ontwerp;
- Een mutatie is een nieuw databaserecord, geen update;
- Mutatielogging werd gebruikt voor selectieprocessen in batchverwerking;
- Op batchprocessen veelal geen mutatielogging, maar verwerkingsverslagen en backup/rollback-mogelijkheden.

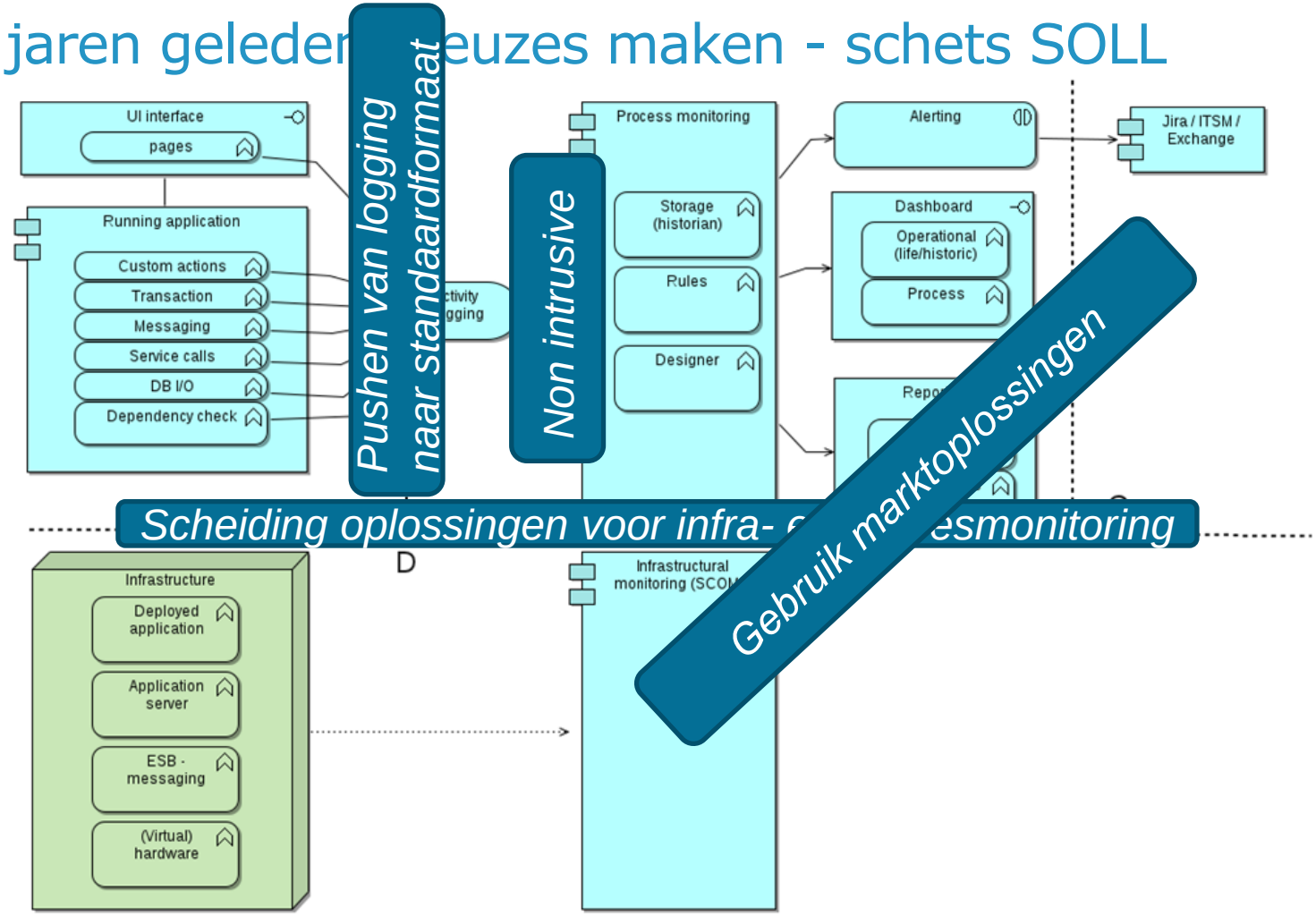
Eind jaren 80: inzet 4GL en AS400

- Kenmerk: OS & DBMS waren geïntegreerd
- Transactielogging is onderdeel van AS400
- Transactielogging geschikt voor rollback, maar ook uitleesbaar

Medio jaren 00: Java i.c.m. DBMS op iSeries

- Automatische transactielogging;
- Expliciete aandacht voor mutatielogging in ontwerp: auditcontext (wie, wanneer, waarmee) bij iedere mutatie;
- Meldingenadministratie (kanaalonafhankelijk)

Enige jaren geleden keuzes maken - schets SOLL

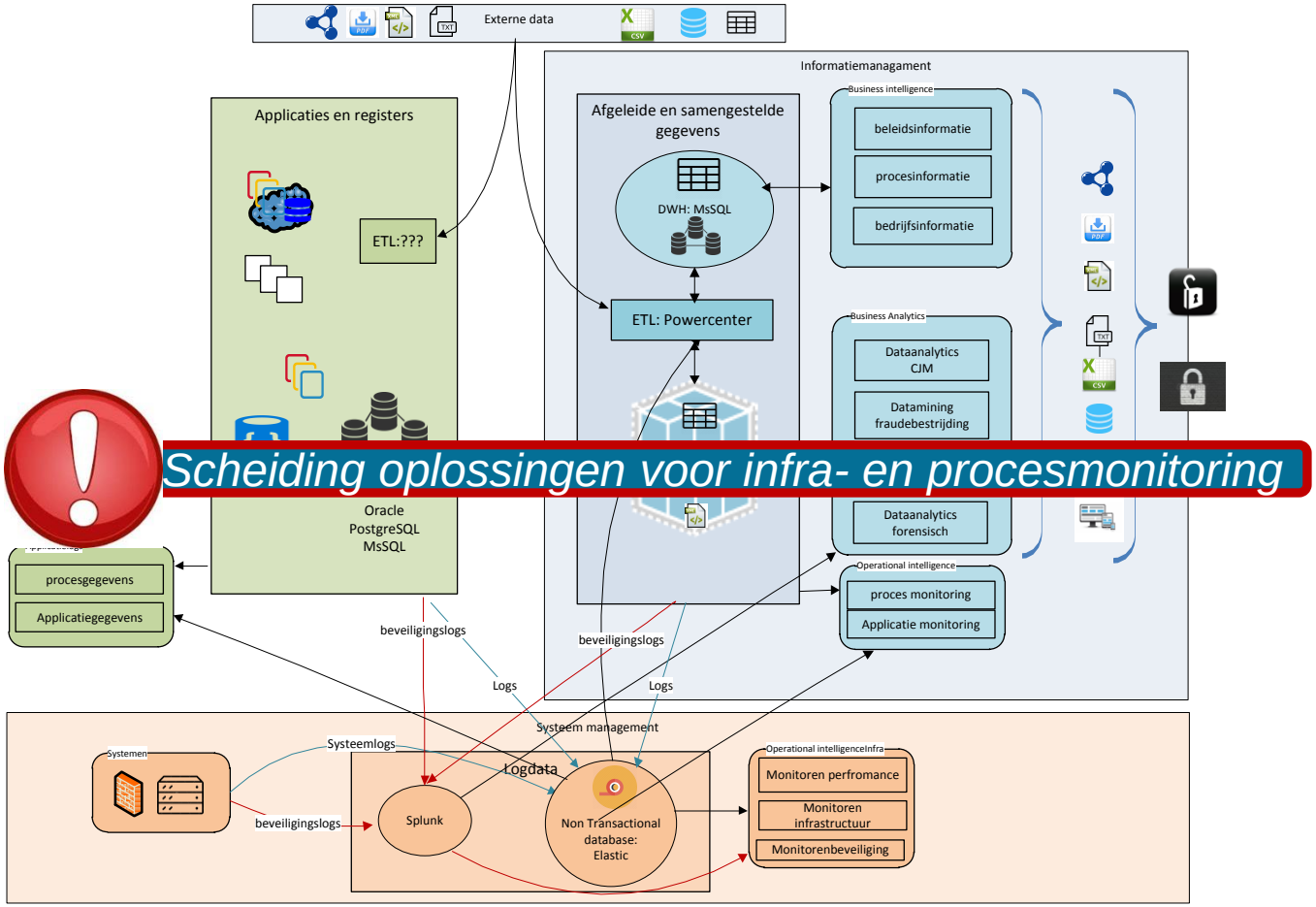


Complexiteit, volume & gebruik neemt toe

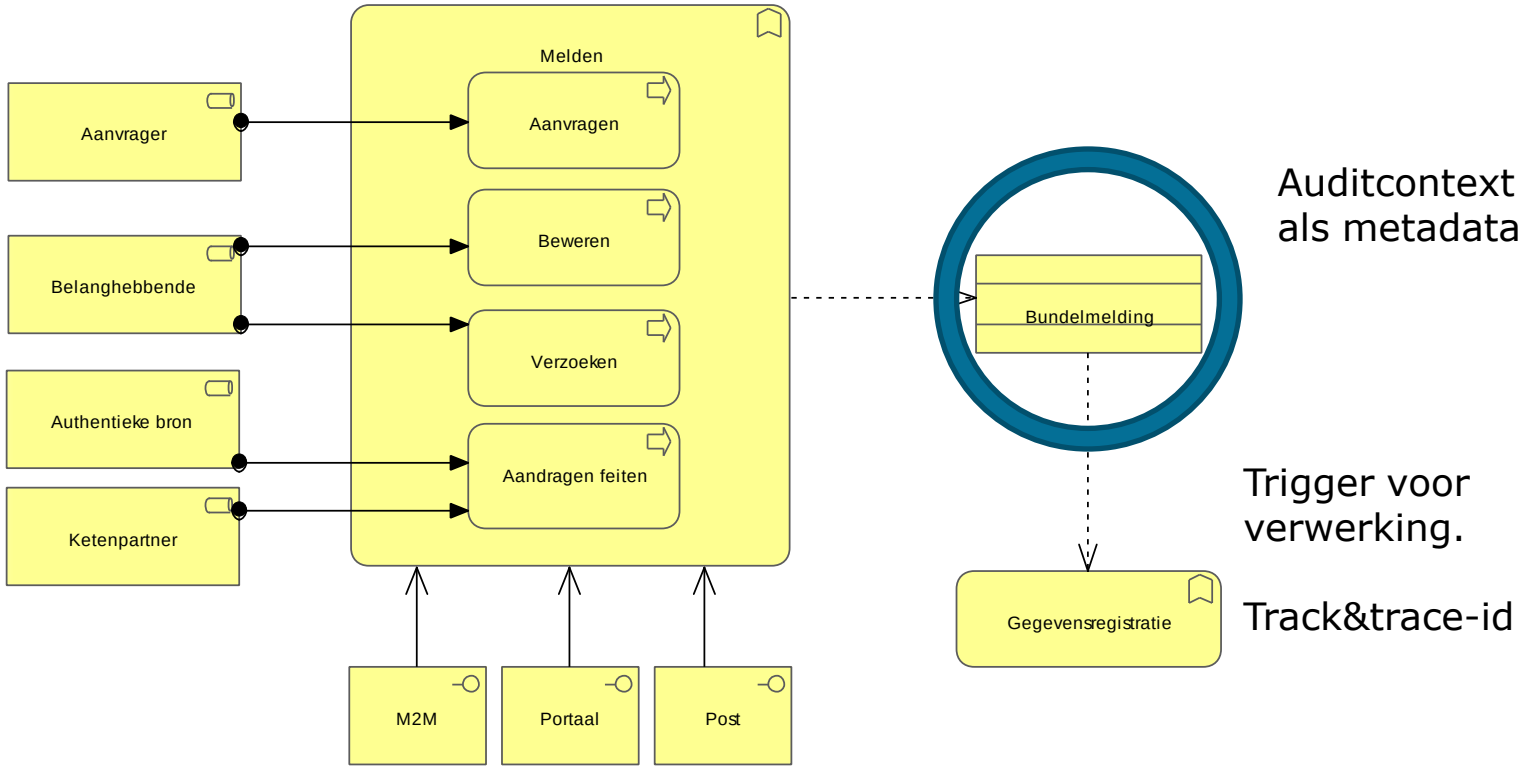
Naast mutatielogging:

- Netwerk monitoring
- Intrusion detection
- Applicatiemonitoring
- Procesmonitoring
- eventlogging
- Performance monitoring
- Website monitoring
- Data mining & analyse
- User experience performance monitoring
- Customer journey mining
- Privacy / anonimisering
- ….

In onderzoek: huidige verkeersstromen



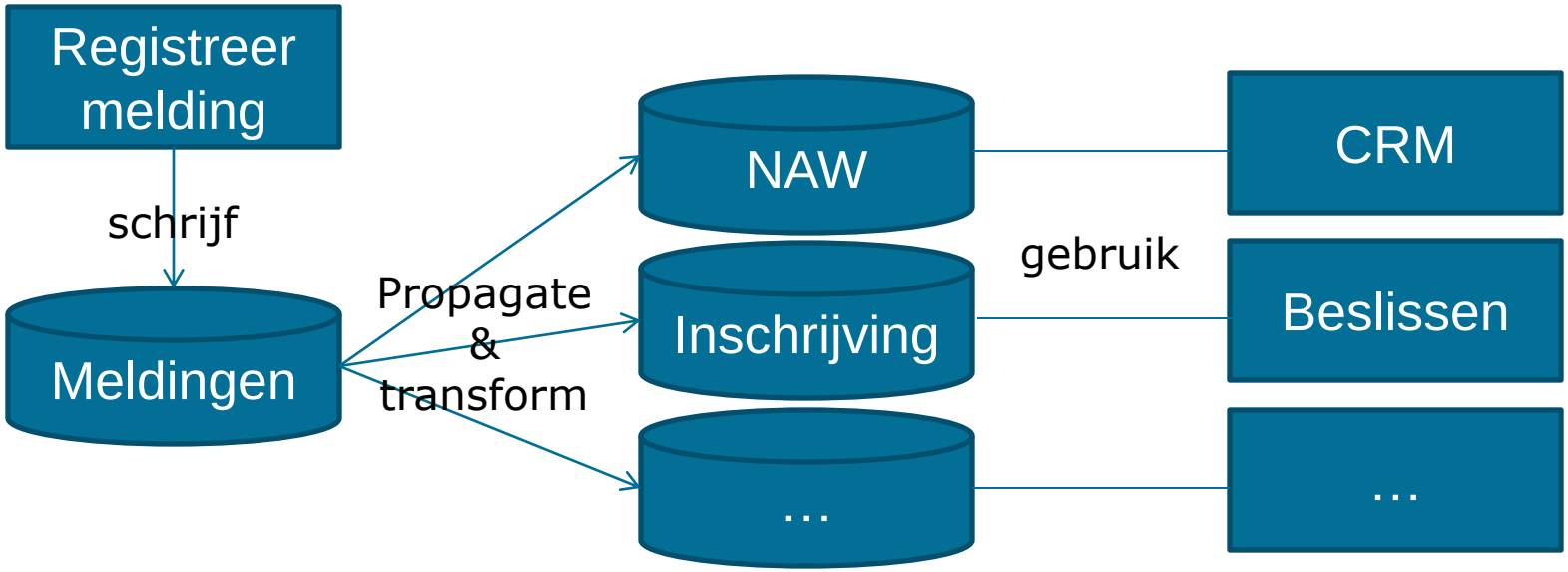
Kanaalonafhankelijke meldingenadministratie: onweerlegbaar bewijs



Terug naar “by design”

In de toekomst:

- melding als “golden record”
- toepassing CQRS-principe
- Vastlegging van bewering is niets anders dan transformatie van melding voor een gebruiksdoel.



Tijd voor vragen