Миграция озера данных с Elastic Stack (ELK) на Smart Monitor

ИТ-мониторинг | Безопасность | Бизнес

Цели

уменьшение стоимости владения (TCO) системы мониторинга, расширение возможностей поисковой аналитики по озеру данных. Сокращение времени и затрат на доработку и развитие проектов по анализу машинных данных.

Задачи

- оптимизация стоимости лицензий на систему мониторинга
- сохранение инфраструктуры сбора и модели/схемы данных
- снижение нагрузки на персонал за счет упрощения анализа данных
- уменьшение количества аппаратных ресурсов, утилизируемых системой
- дообработка событий в процессе запроса за счет конвейерного выполнения
- объединение событий от разных хранилищ данных в едином запросе со сложной логикой

Результаты

Smart Monitor

- до 150% CPU
- до 400% RAM
- до 800% HDD/SSD

- применение гибридного хранилища позволяет снизить аппаратные требования
- сокращение длительности проекта за счет применения готовых модулей платформы
- снижение временных затрат на разработку поисковых запросов на 70%
  - сокращение длины поискового запроса в 4 раза
  - увеличение количества операций над данными в одном запросе в 6 и более раз
- переиспользование имеющейся инфраструктуры сбора данных
- снижение стоимости лицензии в три раза

elastic