ПЕРША ДЕРЖАВНА СИСТЕМА

Система управління процесами, розподілене сховище та телекомунікаційний фреймворк для автоматизації державних підприємств

Максим Сохацький

Київ, 23 вересня 2022

Зміст

Розділ 1

Фреймворк

По аналогії зі стандартом ISO 42010, фреймворк ДП «ІНФОТЕХ» визначає та уточнює архітектурні рівні з яких складаються сучасні корпоративні інформаційні системи:

— Юридично-документальний рівень — Обліково-реєстровий рівень — Зв'язність людей та пристроїв — Телекомунікаційна платформа — Схема та метаінформація — Безпека інтернету

1.1 Юридично-документальний рівень

Згідно фреймворку верхній шостий рівень визначає BPMN процеси згідно яких здійнюється відзеркалення юридично-правивих відносин електронного документообігу. Кожен крок такого процесу, та усі його документи підписуються особистим ключем КЕП посадової особи, що дає змогу проведення диспутів та розслідувань Міністерством юстиції України. Окрім того цей рівень системи орієнтований на аналітику у взаємодії з громадянами через СЕВ ОВВ.

У 2022 році юридично-документальні системи ERP.UNO будуються на сховищі з єдиним простором ключів Facebook RocksDB, що здатне працювати через Intel SPDK на NVMe дисках, наприклад у складі таких сховищ як CEPH. Обсяг обігу документів на великих підприємствах сягає 1ТБ на рік.

1.2 Обліково-реєстровий рівень

Обліково-реєстровий рівень пропонує низькорівневе масштабоване розподілене журнальне сховище даних та метаданих, яке може бути побудоване на реляційних базах даних, базах даних з єдиним простором ключів з гарантіями консистентності (chain-hash) або їх комбінаціях.

Класичні представники цього рівня в системах управління підприємствами: система управління людськими та матеріальними ресурсами, банківські системи PCI DSS, складські системи, системи управління поставками та виробництвом, системи сервісних послуг, системи управління проектами, тощо.

1.3 Зв'язність людей та пристроїв

Рівень зв'язності людей та пристроїв визначає комунікаційні протоколи та технології, які об'єднують головні ресурси підприємства (пристрої та людей) у одну телекомунікаційну мережу. Як правило виробництво складається з багатьох пристроїв що підключаються до промислових шин як MQTT, та робочих місць користувачів.

З точки зору продуктів цей рівень представляється зазвичай корпоративними комунікаторами та дашбордами де здійнюється моніторинг роботизованого обладнання: пристрої, датчики, тощо. Ресурси підприємства — люди та пристрої як правило зберігаються в LDAP директорії підприємства.

1.4 Телекомунікаційна платформа

Рівень платформи визначає засоби мастшабування пам'яті (персистентної та волатильної) та обчислювальних ресурсів (за допомогою процесінгових брокерів доставки повідомлень). Це рівень визначає реляційні бази даних та бази даних з єдиним простором ключів, а також стандарти та протоколи передачі інформації у промислових ERP системах, такі як CSV, JSON, SOAP, BERT, ASN.1, тощо.

1.5 Схема та метаінформація

Рівень схеми даних визначає модель зберігання даних як з точки зору об'єктів-сутностей та і з точки зору технологій та протоколів, які необхідні для їх опису. Головним чином це Фреймворк Закмана та сімейство стандартів які описують UML.

1.6 Безпека інтернету

Рівень безпеки визначає схему функціонування основного центрального засвідчувального орнагу, акредитованих центрів сертифікації ключів, протоколи шифрування та підпису, директорію підприємства, інтернет протоколи найменування ресурсів. Усе визначено згідно ASN.1 специфікації. Компанія ІНФОТЕХ є утримувачем та автором усіх імплементації.

Розділ 2

Специфікація та сертифікація

Розділ 3

Юридично-документальний фреймворк ERP.UNO

3.1 Вступ

Друге видання КНИГИ ERP (англ. ERP BOOK VOL.3 Blue Book) визначає формальну бізнес специфікацію та її імплементацію для сучасних оптимізованих підприємств. Системи ERP на її базі також уже не один рік використовується у банківській сфері, процесінгу транзакцій, розподілених системах повідомлень, в IoT секторі.

3.2 Модулі підприємства

ERP.UNO є комплексом бібліотек (N2O.DEV) та підсистем додатків (ERP.UNO), який використовує загальну шину і загальну розподілену базу даних для швидкіснх операційних вітрин.

LDAP — Сервер аутентифікації, зберігання ключів та директорія підприємства.

ERP — Даний модуль зберігає основну ієрархічну структуру підприємства, її схему, записи про персонал, інвентар, компанії та офіси підприємства.

FIN — Фінансовий модуль підприємства, зберігає бізнес процеси, які представляють собою рахунки учасників системи: персонал (для нарахування зарплат), рахунки та субрахунки підприємства (для здійснення економічної діяльності) і зовнішні рахунки в платіжних системах.

ACC — Система управління персоналом: зарплатні відомості, календар підприємства, відпустки, декретні відпустки, інші календарі.

SCM — Система управління ланцюжком поставок: головний БП системи — експедиційний процес доставки товарів ланцюжку одержувачів за допомогою транспортних компаній.

CRM — Система управління клієнтами: являє собою розширення більш абстрактного додатку CHAT.

PLM — Система управління життєвим циклом проектів і продуктів. Також містить CashFlow та P38;L звіти.

PM — Система управління проектами підприємства з деталізацією часу і протоколів прийому-передачі (прийняті коміти в гитхабі).

WMS — Система управління складом.

TMS — Система управління транспортом підприємства.

3.3 Управління ресурсами

Головним чином інформаційна структура нашого підприємства складається з обчислювальних ресурсов (додатки, запущені в шині) та накопичувальних ресурсів (дані, збережені в базі даних). SOA архітектура в якості моделі управління обчислювальними ресурсами пропонує асинхронний протокол віддаленого виклику на шинах. Разом з N2O можно використовувати MQTT та інші шини, за допомогою наступних протоколів: TCP, WebSocket. Ці асинхронні протоколи часто називають протоколами реального часу, оскільки в них функції відправки повідомлень завжди миттєво повертають результат. Що ж стосується протоколів для публікації і доступу до даних, то тут може виявитися доречним використання синхронного HTTP протоколу.

3.4 Обчислювальні ресурси

Для SOA архітектури традиційно використовуються асинхронні протоколи доступу до обчислювальних ресурсів. Зазвичай це серверні воркери, які підключені до шини і обслуговують API певного додатку. Кожен додаток має власне консистентне хеш-кільце воркерів. В мережі одночасно працює багато кілець-додатків.

```
config :n2o,
  tcp_services: ['ldap'],
  ws_services: ['chat'],
  mqtt_services: ['erp', 'bpe']
```

за допомогою config.exs файлу можна налаштувати необхідну конфігурацію серії консистентних кілець, кожне з яких працює на власному транспортному протоколі. В даному прикладі показано карту Erlang серверів, які обслуговують черги додатків в шині:

```
> PLM.vnodes
[
  {{:tcp, '/ldap/tcp/4'}, [:n2o_tcp]},
  {{:tcp, '/ldap/tcp/3'}, [:n2o_tcp]},
  {{:tcp, '/ldap/tcp/2'}, [:n2o_tcp]},
  {{:tcp, '/ldap/tcp/1'}, [:n2o_tcp]},
  {{:ws, '/chat/ws/4'}, [:n2o_ws]},
  {{:ws, '/chat/ws/3'}, [:n2o_ws]},
  {{:ws, '/chat/ws/2'}, [:n2o_ws]},
  {{:ws, '/chat/ws/1'}, [:n2o_ws]},
  {{:mqtt, '/erp/mqtt/4'}, [:n2o_mqtt]},
  {{:mqtt, '/erp/mqtt/3'}, [:n2o_mqtt]},
  {{:mqtt, '/erp/mqtt/2'}, [:n2o_mqtt]},
  {{:mqtt, '/erp/mqtt/1'}, [:n2o_mqtt]},
  {{:mqtt, '/bpe/mqtt/4'}, [:n2o_mqtt]},
  {{:mqtt, '/bpe/mqtt/3'}, [:n2o_mqtt]},
  {{:mqtt, '/bpe/mqtt/2'}, [:n2o_mqtt]},
  {{:mqtt, '/bpe/mqtt/1'}, [:n2o_mqtt]},
  {{:caching, 'timer'}, [:n2o]}
]
```

Завдяки такій деталізації можна проектувати гетерогенні системи, включаючи необхідний набір протоколів на портах потрібних машин. Ця же система дозволяє отримати балансування навантаження, підключаючи фізичні ресурси до певних черг шини даних.

В нашій моделі асинхронні протоколи використовуються для управління обчислювальними ресурсами підприємства.

3.5 Накопичувальні ресурси

Розподілені хеш-кільця використовуються не тільки для розподілених обчислень, але і для зберігання даних. Деякі бази даних, наприклад RocksDB та Cassandra, використовують глобальний простір ключів для даних (на відміну від таблично-орієнтованих баз). Саме для таких баз і створено библиотеку KVS, де в якості синхронного транзакційного інтерфейсу — API ланцюжків з гарантією консистентності. Нижче наведено приклад структури ланцюжків екземпляру системи PLM:

```
> :kvs.all :writer
[
  {:writer, '/bpe/proc', 2},
  {:writer, '/erp/group', 1},
  {:writer, '/erp/partners', 7},
  {:writer, '/acc/synrc/Kyiv', 3},
  {:writer, '/chat/5HT', 1},
  {:writer, '/bpe/hist/1562187187807717000', 8},
```

```
  {:writer, '/bpe/hist/1562192587632329000', 1}
]
```

В нашій моделі синхронні протоколи використовуються для управління накопичувальними ресурсами підприємства і транзакційного процесингу.

3.6 Типові специфікації

Протоколи визначаються типовими специфікаціями і генеруються для наступних мов: Java, Swift, JavaScript, Google Protobuf V3, ASN.1. Також ми генеруємо валідатори даних по цих типових анотаціях і вбудовуємо ці валідатори в тракт наших розподілених протоколів, тому ми ніколи не дозволимо клієнтам зіпсувати сторадж. Для веб додатків у нас развинута система валідації — як для JavaScript, так і на стороні сервера. Бізнес логіка повністю ізольована в нашій системі управління бізнес процесами, де кожен бізнес процесс є процесом віртуальної машини. Всі ланцюжки модифікуються атомарним чином, підтримують flake адресацію, і не вимагають додаткової ізоляції у своєму примітивному використанні. Тому ви можете трактувати базу як розподілений кеш і використовувати її з фронт додатків для примітивних випадків.

Розділ 4

Технологічна платформа N2O.DEV

4.1 Вступ

Архітектурна компанія SYNRC розробляє та підтримує систему автоматизації підприємства N2O.DEV, побудовану згідно формальної специфікації яка призначена для розробки багатофункціональних гетерогенних платформ для додатків та сервісів на основі шини та розподіленої бази даних. N2O.DEV уже використовується у банках, системах повідомлень, державних підприємствах та інших менших чисельних організаціях в Америці, Європі та Азії.

Друге видання КНИГИ N2O (англ. N2O BOOK Vol. 2 Green Book) визначає форамальну специфікацію на програмне забезпечення усіх рівнів моделі Закмана для підприємств ISO-42010, містить широкий спектр прикладів, розказує про складові компоненти та є вичерпним авторським стартовим посібником для курсу навчання розробки технологічних програм для платформи Erlang.

4.2 Структура виробничого процесу

4.3 Ланцюжки BTree

4.4 Сховище NVMe

4.5 Логіка BPMN

4.6 Додатки

Розділ 5

Результати

ЄРЗ (Єдиний реєстр зброї НПУ), СУСЗЦЗ (Система управління силами та засобами цивільного захисту ДСНС), ЄІС (Єдина інформаційна система МВС), ФП МТРЗ (Функціональна підсистема матеріально-технічного та ресурсного забезпечення МВС), ГСЦ (Головний сервісний центр МВС).