

ORACLE®

Москва, «Инфофорум-Евразия», Июнь 2010 г.

«Подход к обеспечению безопасности на транспорте и системы обеспечения безопасности на транспорте»

Игорь Маврин — руководитель сектора “Транспорт”, Sun Microsystems
Алексей Задонский – ведущий специалист, Oracle CIS

ORACLE®

Лидер на ключевых рынках



- База данных
- База данных на Linux
- ПО разработки
- ПО промежуточного уровня
- Управление взаимоотношениями с клиентом
- Производство и продажа ТНП
- Телеком
- Подбор и развитие персонала
- Финансовый сектор
- Банки
- Государственный сектор
- Обучение
- Управление эффективностью бизнеса
- Хранилища данных

Объединение возможностей



О чем сегодня пойдет речь:

Первая часть.

Формулировка “ключевой” проблемы построения систем безопасности как мы ее себе видим.



Вторая часть.

Способ решения поставленной задачи средствами Oracle.



Что такое безопасность?

Безопасность — это такое состояние *сложной системы*, когда действие внешних и внутренних факторов не приводит к ухудшению системы или к невозможности её функционирования и развития



Базовые технические условия

Большое количество разрозненных источников информации



Механизмы
причины

Необходимо предусматривать механизмы интеграции!!!



Необходимость быстрого (реал-тайм) и адекватного реагирования на события или группы событий



Базовые организационные принципы



Необходимо предусматривать механизмы описания и исполнения процедур принятия решения!!!

задача

Подведение итогов и подготовка отчетных документов

отчет

Контроль и помощь в ходе выполнения задач

Организация всестороннего обеспечения

Предоставить правильные данные - правильным людям - в нужное время!!!

- ▶ Содействие в образовании “специальной сети” между основными службами обеспечивающими безопасность



- ▶ Управление данными и их сравнение из всех доступных источников
- ▶ Единая среда взаимодействия и коммуникационная инфраструктура обеспечивающая доступность ключевой информации
- ▶ Механизм идентификации ключевой информации и оценки ее значимости

Стек продуктовой линейки Oracle

Исчерпывающий

Открытый

Единый



- ❖ Единая разработка
- ❖ Совместное тестирование
- ❖ Совместная сертификация
- ❖ Единая “упаковка”
- ❖ Совместное развертывание
- ❖ Совместное обновление
- ❖ Единое управление
- ❖ Единая поддержка

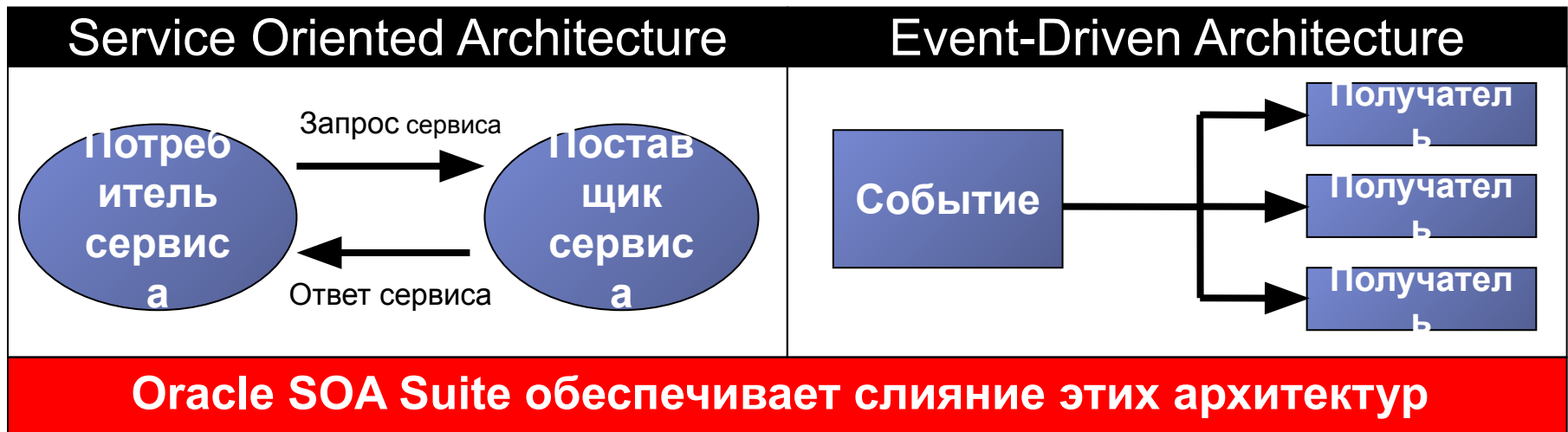
The background features a white-to-gray gradient with a perspective grid pattern. A solid red horizontal band is positioned in the middle. The text is centered on the right side of the red band.

Вторая часть.

Алексей Задонский

Сервисно-ориентированная архитектура

- ❖ **Service-Oriented Architecture (SOA)** - это архитектура, в которой система строится из набора слабосвязанных компонентов (сервисов)
- ❖ **Event-Driven Architecture (EDA)** - это архитектура, в которой система строится на основе взаимодействия компонентов по событиям

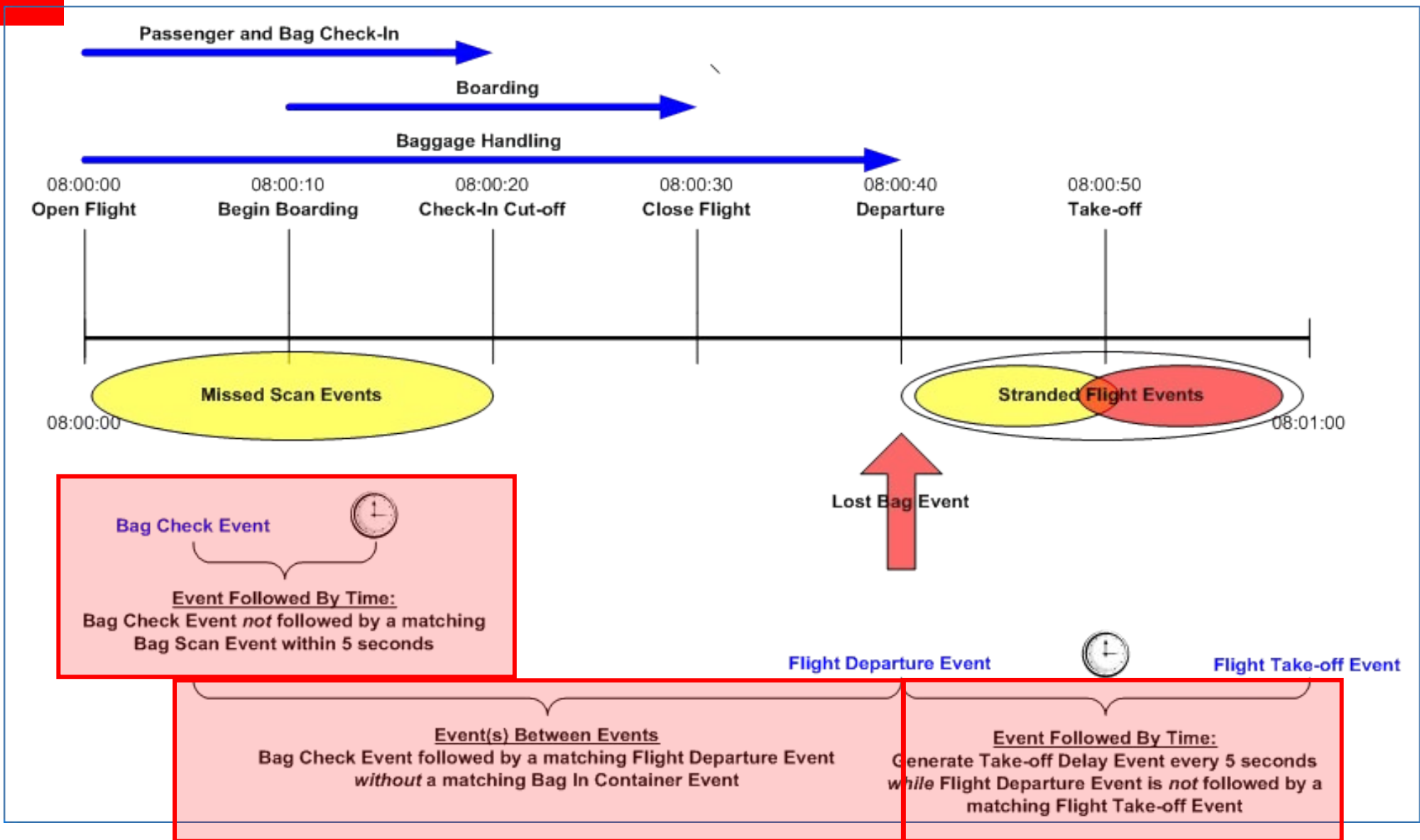


Зачем нужна обработка потоков событий



- ❖ Непрерывный поток, часто большого объема
- ❖ Отсутствует конец потока
- ❖ Упорядочен по времени
- ❖ Нужно на лету уметь обнаруживать «шаблоны»
- ❖ Невозможно или не эффективно обрабатывать/анализировать в реальном времени с применением баз данных

Временной сценарий и шаблоны событий



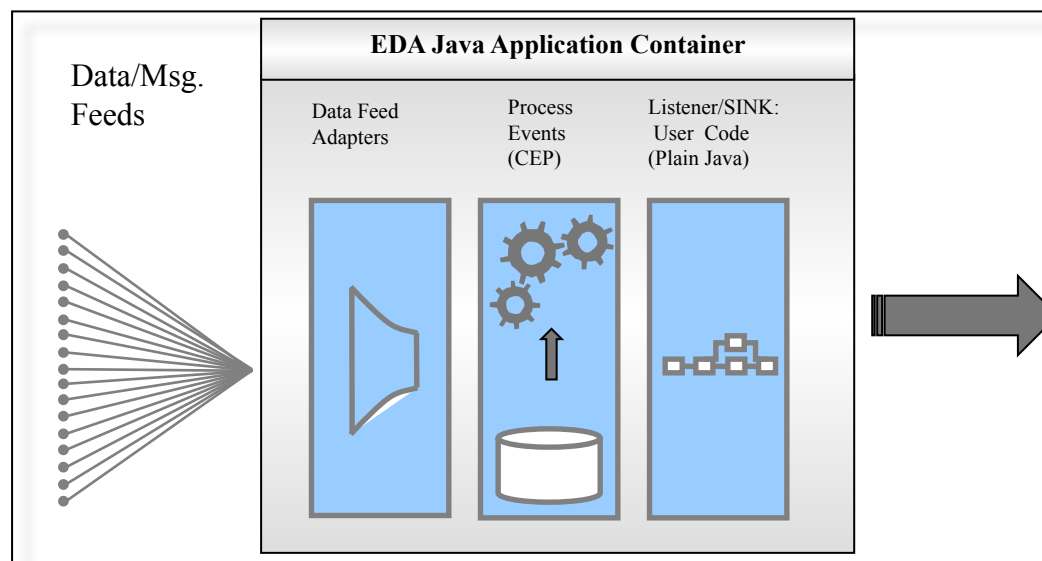
Новый язык запросов – CQL

Continuous Query Language

- ❖ Расширение распространенного языка SQL поддержкой непрерывно действующих запросов. Использование реляционных операторов для работы с потоками
 - Фильтрация, агрегация, корреляция событий
- ❖ Готовится к принятию в качестве стандарта
- ❖ Поддержка разных сценариев, обнаружение шаблонов событий, обнаружение пропущенных событий и т.д.
- ❖ Множество успешных реализаций

Сервер - Oracle Event Server (CEP)

быстрый и «легкий» сервер обработки событий



Фильтрация, агрегация, корреляция событий
Возможность обрабатывать более 1,000 запросов

Входной поток данных
1,000,000 событий/сек.
Размер сообщения < 1К

Задержка
< 1 Millisecond Latency (Avg.)
10 Millisecond Latency (Max)

Выходной поток событий
< 5% событий входного потока
удовлетворяет критерию

Успешное внедрение Oracle CEP

Thomson Financial



Thomson создает качественные независимые обзоры новостных лент и другой контент для принятия решений при торговле на финансовых рынках. Выручка \$7.4 млрд.

Задачи:

- Мониторинг огромного потока информации (от 100,000 до 200,000 сообщений в сек., задержка < 10ms)
- Идентификация того, кто может быть заинтересован в информации с учетом безопасности
- Маршрутизация только заинтересованным сторонам
- Сохранения в распределенном кэше для дальнейшего использования

Работает на платформе:

- Event Server: IBM 335s с 2 Xeon (2.8 GHz) и 4 GB RAM, под управлением 32-bit RedHat ES 4.0

Успешное внедрение Oracle CEP

Bear Stearns



Bear Stearns (сейчас в составе JP Morgan) лидер мирового финансового рынка с объемом активов \$1.6 трлн. и деятельностью более чем в 60 странах. Лидер в областях: инвест. и коммерческая банковская деятельность, обработка финансовых транзакций, управление активами.

Задачи:

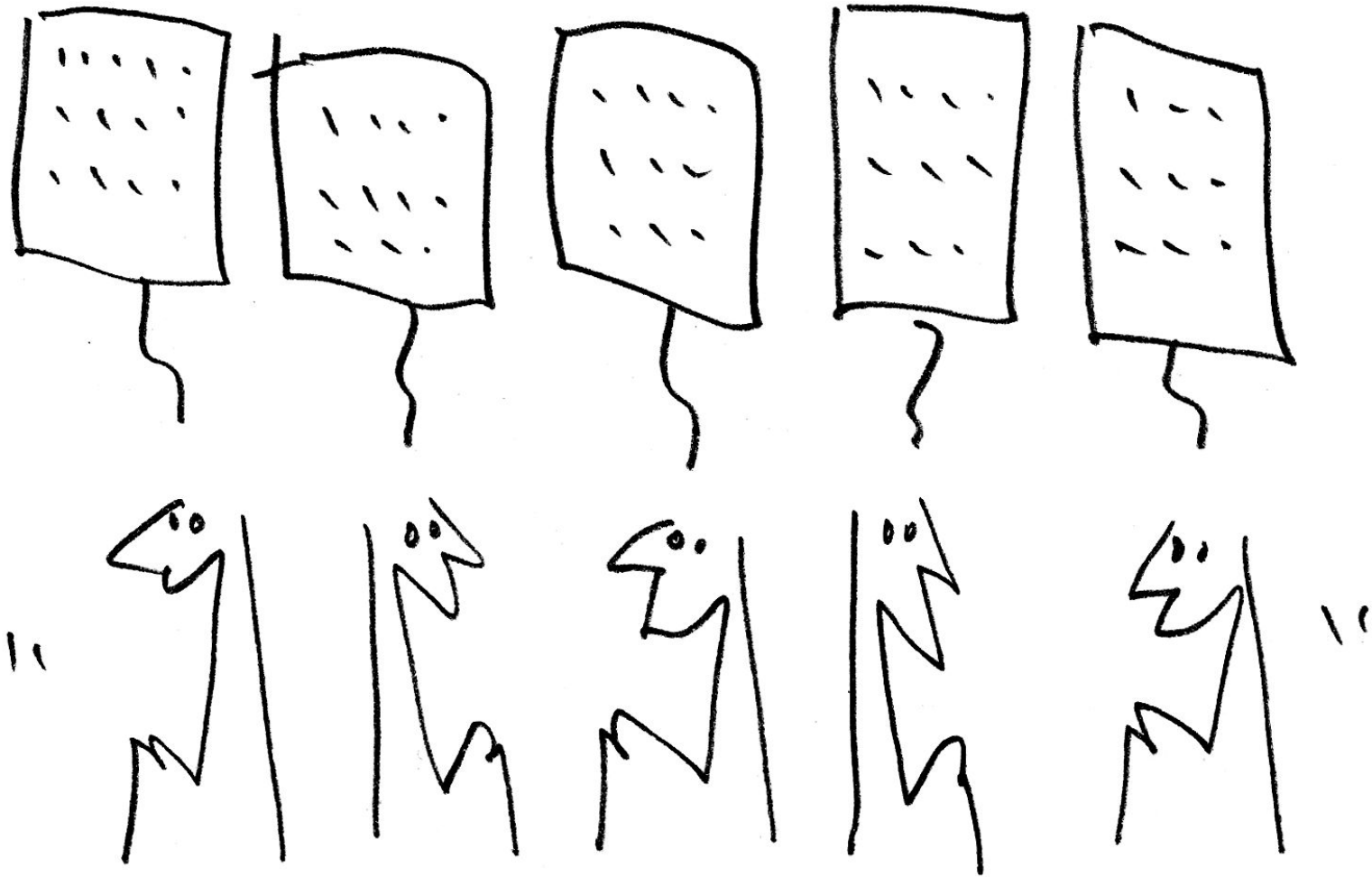
- Поддержка потоков VWAP (Volume Weighted Average Percentage) для рынка Северной Америки
- Обработка первичных финансовых событий
- Расчет VWAP с минутным интервалом для всех котируемых объектов на протяжении всего дня
- Производительность: более 800К событий/сек, задержка менее 1 ms

$$P_{VWAP} = \frac{\sum_j P_j \cdot Q_j}{\sum_j Q_j}$$

Работает на платформе:

- Event Server, IBM System X3650 2 CPU (Intel Xeon по 4 ядра X5350) с 32 GB RAM, под управлением SUSE Linux 10

Вопросы и ответы



SOFTWARE. HARDWARE. COMPLETE.



Спасибо за Внимание!!!