**Интеграция OWSM и BPEL**

Уильям Батерст

**Введение**

Сервис-ориентированная архитектура (SOA - Service Oriented Architecture) – это архитектура программного обеспечения, в которой главенствуют прозрачность местоположения (location transparency) и интероперабильность (interoperability - способность к взаимодействию). Компании рассматривают SOA, как средство для интеграции систем и процессов организаций и партнеров. Чтобы обеспечить масштабирование, слаженность и эффективность функционирования, SOA необходимы некоторые ключевые компоненты. В этой статье описываются два таких важнейших компонентов SOA: Oracle BPEL Process Manager и Oracle Web Services Manager.

BPEL выступает как стандарт компонования множества синхронных и асинхронных сервисов в совместно работающие, согласованные потоки процессов. Это дает преимущество предприятиям, которые желают реализовать свои бизнес-процессы стандартным и переносимым способом, избегая заданных вендом правил, которые не всегда выполнимы.

Oracle BPEL Process Manager (Oracle-менеджер BPEL-процессов) обеспечивает легкое в использовании и надежное решение для проектирования, развертывания и управления BPEL бизнес-процессами. Он включает в свой состав JDeveloper BPEL Designer, который позволяет используя BPEL, моделировать, редактировать, и проектировать бизнес-процессы. Ядро BPEL-механизма обеспечивает самую развитую, масштабируемую и надежную реализацию доступного сегодня BPEL-сервера. BPEL осуществляет управление бизнес-процессами, как SQL - управление данными.

Сущесвует потребность обезопасить эти потоки бизнес-процессов. Например, бизнес-процесс может взаимодействовать с бизнес-партнером по Интернету. Должна быть предписана политика безопасности, чтобы гарантировать безопасность корпоративных данных.

Oracle Web Services Manager (OWSM – Oracle-менеджер Web-сервисов) позволяет компаниям определить политику (образ действий), которая управляет действиями web-сервисов, как-то: доступ, авторизация, регистрация, балансировка нагрузки, а затем свернуть (wrap) эту политику в web-сервисы. Также OWSM осуществляет мониторинг статистики, чтобы обеспечить качество обслуживания, продолжительность работы, выявление угроз безопасности, и показывает ее на своей панели. Эта функциональность теперь может быть применена к бизнес-процессам, управляемым BPEL.

**Защита потоков BPEL-процессов**

Одной из возможностей Oracle Web Service Manager Оракула является способность защитить потоки BPEL-процессов. OWSM защищает BPEL, используя PEP (Gateway Policy Enforcement Point – Шлюзовая точка претворения политики), в который перехватываются SOAP-запросы и выдаются ответы в различные точки BPEL-процесса. Даайте рассмотрим демонстрационный пример Loanflow, приведенный в учебнике BPEL 101 Tutorial, чтобы проиллюстрировать, как OWSM защищает BPEL-процессы. BPEL-пример Loanflow демонстрирует автоматическое получение банковской ссуды:

Заявитель представляет банку на рассмотрение свою заявку.

Банк проводит кредитную проверку заявителя ссуды и получает оценку его кредитоспособности.

Если эта оценка хорошая, то банк направит заявку двум кредитным бюро и выберет лучшее для клиента предложение.

В этом демонстрационном примере “оценка кредитоспособности” - синхронный Web-сервис. BPEL-процесс будет ждать ответ от этого кредитного сервиса перед переходом к следующим шагам. Затем демо-пример начинает параллельный диалог с двумя асинхронными сервисами обработки ссуд (Star Loan и United Loan).

Диаграмма 1. Демонстрационный BPEL-пример Loanflow

Этот сценарий интересен тем, что в нем смоделирован бизнес-процесс, который обращается с конъюнктурные данными (например, номер [карточки] социального обеспечения), но этот бизнес-процесс не защищен. Мы же видим, что:

Нет никакой авторизации или аутентификации, обязательно представляемых каждой заявкой.

Номер Social Security ([карточки] социального обеспечения) заявителя представлен в открытом коде.

Очень важна проверка достоверности сообщения. Например, может статься, что любая ссуда запрашивает свыше ста тысяч долларов.

К BPEL web-сервисам можно обратиться по интернету. Если запрос сначала проходит шлюз, то они должны быть виртуализированы и уже доступны.

Нет никакой журнализации или представления трафика сообщений в течение всего потока.

Этот пример показывает насколько мощной может стать комбинация BPEL и OWSM. OWSM усиливает BPEL за счет:

**Контроля Доступа (Access Control)**

BPEL-процесс может быть защищен, если перед ним поставить шлюз. Только аутентифицированние/авторизированные (authenticated/authorized) пользователи могут начать поток [получения] ссуды. Например, если перед BPEL-процессом находится COREid-шлюз политики аутентификации/авторизации (authentication/authorization), то он позволит проход только привилегированным пользователям. Контроль доступа может также быть применен для отдельных сервисов BPEL-процесса.

Частичного/полного шифрования сервисных запросов (Partial/full encryption of service calls)

Клиент, посылающий запрос к BPEL-процессу, может послать зашифрованное сообщение, и BPEL-процесс должен быть способен расшифровать это сообщение в некоторой точке BPEL-процесса, когда это будет необходимо. BPEL-процесс должен поместить шлюз перед сервисом, который должен получить расшифрованное сообщение.

Клиент имеет возможность послать зашифрованное сообщение, которое должно быть расшифровано в некоторый момент в BPEL-процессе. Если вернуться к демо-примеру Loan, клиент может послать зашифрованное сообщение BPEL-процессу. Web-сервис Loan Flow BPEL-процесса получает зашифрованный запрос. На следующем шаге нужно вызвать сервис, который даст кредитную оценку. Поэтому желательно поместить шлюз, который может расшифровать сообщение, перед этим - Credit Rating Service - сервисом.

DMZ-виртуализации асинхронных BPEL-сервисов (DMZ Virtualization of asynchronous BPEL services)

Архитекторы служб безопасности и web-сервисов часто хотят виртуализировать возврат (callback) к BPEL-процессам. Это означает то, что клиент не должен непосредственно общаться с BPEL-процессом. Вместо этого, возвраты должны проходить через некий модуль доступа (proxy) и только затем быть соответственно маршрутизированы (route). Для подобных запросов OWSM может установить режим шлюза (Gateway mode) и proxy-модуль. Одновременно OWSM также может выполнять и другие интеллектуальные задачи обработки, как-то: проверка достоверности сообщений (message validation), регистрация (logging) и применение дополнительных политик безопасности (extra security policies).

**Мониторинга (Monitoring)**

OWSM-шлюз, который защищает BPEL-процесс, посылает свои данные OWSM-монитору. ИТ-служащие могут использовать монитор, чтобы увидеть в реальном времени в общее состояние, производительность и безопасность BPEL-процесса. Например, по диаграммам аутентификации/авторизации они узнают, какие BPEL-процессы совершили попытки несанкционированного доступа. Используя монитор, ИТ-служащие могут задать правила мониторинга и автоматически получать алерт-сигналы по электронной почте, когда имеют место определеные состояния.

**Анализ бизнес-процессов**

Первый шаг к обеспечению безопасности бизнес-процесса состоит в анализе бизнес-процесс на предмет слабости его безопасности. В случае демо-примера Loanflow мы отметили несколько возможных слабостей и мест, где были бы полезны аудит и мониторинг. Следующая диаграмма являет пример того, как в демо-примере Loanflow может быть развернут OWSM, чтобы обеспечить безопасность этого бизнес-процесса:

**Заключение**

Когда организация начинает реализовывать SOA, она выставляет свои бизнес-функции как сервисы. Эти сервисы, подобно сервису оценки кредитоспособности, затем совместно используются в потоках бизнес-процессов. Oracle предоставляет два ключевых инструментальных средства, чтобы реализовать и развернуть SOA: BPEL и OWSM.

Каждый инструмент играет свою роль: BPEL используется для оркестровки (orchestrate) бизнес-потоков. Например, если потребуются сервисы, типа Credit Rating, Star Loan и United Loan, он оркеструет их в бизнес-процесс. OWSM используется для обеспечения безопасности и мониторинга каждого из этих сервисов в потоке бизнес-процесса. Естественное взаимодействие этих двух инструментальных средств приводит к комплексным решениям, обеспечивая оркестровку и безопасность.