ПРИМЕНЕНИЕ SOA В СУПЕРКОМПЬЮТЕРНЫХ ЦЕНТРАХ

А.С. Лукичев, И.О. Одинцов, А.Ю. Чернышев

Суперкомпьютерные центры перестали быть атрибутом исключительно государственных лабораторий и крупнейших университетов и, благодаря быстрому развитию аппаратного обеспечения, находят все более широкое применение в науке, образовании, на производстве, здравоохранении, в сфере финансов и т.д. Использование сервис-орентированной архитектуры и облачных вычислений требует подключения суперкомпьютерного центра к сети Интеренет. Это, в свою очередь, делает центр подверженным сетевым атакам, особенно, если те или иные ресурсы центра доступны в виде сервисов. Таким образом, организация эффективной работы суперкомпьютерных центров подразумевает не только оптимальный дизайн аппаратной части и точную настройку основного программного обеспечения, но и использование высокопроизводительных и надежных вспомогательных компонентов, отвечающих за обеспечение сетевой безопасности, маршрутизацию сообщений, виртуализацию и интеграцию сервисов вычислений и данных.

К задачам обеспечения сетевой безопасности можно отнести следующие:

- автоматическое распознавание и пресечение сетевых атак;
- аутентификацию и авторизацию пользователей и сетевых сущностей, обращающихся к сервисам центра;
- шифрование сообщений;
- федерацию идентификаторов ползователей, поддержку однократного логина.

Маршрутизация сообщений, как правило, заключается в перенаправлении сообщения целевому сервису на основе информации, содержащейся внутри сообщения или в его заголовках. При этом внутренняя архитектура центра оказывается скрытой для внешнего мира, что, с одной стороны, обеспечивает дополнительный уровень безопасность, а с другой, является элементом структурной декомпозиции, повышает управляемость инфраструктуры, масштабируемость предоставлеямых сервисов.

Виртуализация и интеграция сервисов вычислений и данных позволяют получить качественно новые сервисы на основе уже развернутых в суперкомпьютерном центре.

Важно отметить, что перечисленные области не являются изолированными друг от друга. Так, например, зачастую перечисленные выше задачи обеспечения сетевой безопасности решаются различными компонентами, возможно, различных производителей. Сопряжение таких компонент можно, таким образом, отнести к задачам интеграции. С другой стороны, интеграция сервисов подразумевает не только преобразование синтаксиса сообщений или смену сетевого протокола, но и изменение формата и набора атрибутов сетевой безопасности, идентифицирующих сообщения (к примеру, проверку идентификатора и пароля пользователя, посланных в сообщении, и снабжение сообщения цифровой подписью центра для дальнейшей пересылки).

Несмотря на различные проблемные области перечисленные выше задачи имеют общие аспекты, такие как:

- необходимость обеспечения высокой пропускной способности, минимизации задержки сообщений. Это требование особенно существенно в связи с тем, что суперкомпьютерные центры, как правило, создаются под большую нагрузку;
- высокопроизводительная обработка XML. XML - де-факто стандарт представления данных, причем наибольшее применение находит именно в протоколах взаимодействия сервисов. К обработке XML можно отнести возможность выполнения запросов XPath и преобразований XSLT;
- масштабируемость - вспомогательные компоненты не должны ограничивать потенциальное развитие суперкомпьютерного центра и увеличение его нагрузки;
- управляемость - каждая решающая одну из перечисленных задач компонента должна иметь возможность дополнительной настройки, причем количество конфигурируемых параметров (в широком смысле) весьма велико. Удобство настройки каждой компоненты и всего их комплекса в целом отражается не только на производительности труда системных администраторов центра, но и на надежности работы системы, уменьшая вероятность влияния "человеческого фактора".

Развитие технологий параллельной обработки данных происходит по нескольким направлениям, что обусловлено различными потребностями основных потребителей, в частности: системами управления экономикой предприятия и приложениями математического моделирования. В то же время, актуальной становится задача налаживания взаимодействия бизнес-сервисов и средств моделирования. Действительно, часто общим ресурсом систем обоих типов являются входные данные, такие как: геоинформация, каталоги изделий и деталей, статистическая информация и т.д. В рамках предприятия имеет смысл поддерживать единую базу таких данных. Но при этом приходится решать вопросы определения интерфейса доступа к данным и защиты данных от несанкционированного доступа. Наилучшим решением здесь является применение сервис-ориентированной архитектуры (SOA) ПО. В то же время, в задачах, где происходит обработка больших массивов данных (моделирование, выборки и т.п.), скорость работы такого SOA-интерфейса к БД является

критической характеристикой. Решением может служить применение сервис-маршрутизатора (Service Router) – специального устройства или ПО, решающего задачи:

- первичного анализа и фильтрования входящих сообщений;
- маршрутизации сообщений к backend-сервисам;
- нормализации содержимого сообщений;
- нормализации данных для подсистемы безопасности.

При этом в задачи сервис-маршрутизатора входит, в основном, синтаксическая обработка сообщений, что оставляет бизнес-логику backend-сервисам и позволяет увеличить производительность. Выделение вопросов формата сообщений (например, протокол) и данных подсистемы безопасности, которые, вообще говоря, ортогональны бизнес-логике, из backend-сервисов не только снижает затраты на их разработку и поддержку, но и позволяет лучшим образом распределить роли в управлении информационной системой. Подсистема маршрутизации позволяет сервис-маршрутизатору служить также балансировщиком нагрузки.

Благодаря узкому кругу решаемых задач и применению для них специализированных алгоритмов и аппаратных средств (например, устройства аппаратного шифрования), сервис-маршрутизатор может демонстрировать высокую производительность. Таким образом, концепция сервис-маршрутизатора может стать существенным элементом архитектуры суперкомпьютерных центров.