К. В. Карман, Ю. М. Туманов

МОДЕЛЬ СЕРВЕРА ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ, РЕАЛИЗУЕМЫХ НА ГРИД-СЕТИ

В настоящее время растет необходимость во все большем количестве вычислительных ресурсов и постоянном доступе к информации. Для решения данной проблемы все чаще используется относительно новая технология облачных вычислений (ОВ), несущая в себе новые физическую инфраструктуру и технологию виртуализации. Облачные вычисления — это модель обеспечения повсеместного и удаленного доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов, которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами и (или) обращениями к поставщику [1].

Наиболее распространенным подходом к развертыванию сред облачных вычислений с точки зрения аппаратного обеспечения является использование вычислительных кластеров. Облачные вычисления продолжают развиваться, приводя к росту вычислительных нагрузок, созданию новых приложений и новых подходов к их реализации. По оценкам, приведенным в [2], массовое распространение технологии ОВ начнется в 2012—2013 годах. Причем дальнейшее развитие технологии ОВ будет необходимо обеспечивать без повышения эксплуатационных расходов или сложности администрирования. Также необходимо, чтобы технология ОВ соответствовала всем требованиям информационной безопасности.

Предлагаемый подход к развертыванию сред облачных вычислений

При создании новых подходов к развертыванию сред ОВ необходимо обеспечить решение следующих задач [3]:

- доступность и эффективность предлагаемого подхода;
- стабильность работы критически важных приложений внутри среды ОВ;
- безопасность и конфиденциальность данных в общедоступной среде ОВ;
- выбор решений, обеспечивающих гибкость и совместимость.

Был проведен анализ существующих подходов к развертыванию сред ОВ, на основе результатов которого было принято решение о создании нового подхода, учитывающего выявленные в ходе анализа преимущества и недостатки. В качестве программно-аппаратной платформы, используемой для развертывания среды ОВ, предлагается использовать специально разработанную реализацию Грид-сети (далее среда облачных вычислений, реализуемых на Грид-сети — среда ОВГ).

Схема работы предлагаемого подхода к развертыванию сред ОВ

В отличие от существующих подходов к развертыванию сред ОВ, в новом вычислительным узлом является средство вычислительной техники (СВТ) пользователя, на котором установлено программное обеспечение (ПО), включающее в себя: клиента ОВГ и клиента Грид-сети. Клиент ОВГ отвечает за предоставление ресурсов среде ОВГ, обеспечение целостности и конфиденциальности обработки данных при выполнении задания. Клиент Грид-сети обеспечивает функционирование клиента ОВГ и отвечает за взаимодействие клиента ОВГ и сервера ОВГ.

Координатор ОВГ, входящий в состав сервера, выполняет функции, связанные с компонентами, формирующими среду ОВ, а менеджер приложений — функции, связанные с Грид-сетью.

Функциональные возможности и алгоритм работы сервера

Компонентом, отвечающим за координацию взаимодействий составляющих предлагаемого подхода, является сервер среды ОВГ — логически объединенная группа модулей, ответственных за взаимодействие с пользователями среды ОВГ, обработку заданий перед передачей в Грид-сеть

для вычислений, а также за сбор, проверку на достоверность, хранение и передачу результатов пользователям.

Сервер среды ОВГ состоит из следующих компонентов, изображенных на рис. 1:

- Координатор — совокупность программных модулей, обеспечивающих: мониторинг состояния вычислительных узлов и клиентов Грид-сети; проведение распараллеливания и сбалансированного распределения задач между клиентами Грид-сети; сбор, хранение и передачу достоверных результатов внутри среды распределенных вычислений;
- Менеджер приложений среды ОВГ — совокупность программных модулей, обеспечивающих: загрузку и обновление программного обеспечения для распространения внутри Грид-сети; компиляцию/интерпретацию кода в соответствии со спецификацией системы; аутентификацию пользователей среды ОВГ; верификацию задач перед передачей в Грид-сеть для вычисления;
- Координатор безопасности — модуль, отвечающий за обеспечение безопасности внутри среды ОВГ, использующий инфраструктуру открытых ключей (PKI) и механизм электронно-цифровой подписи (ЭЦП).

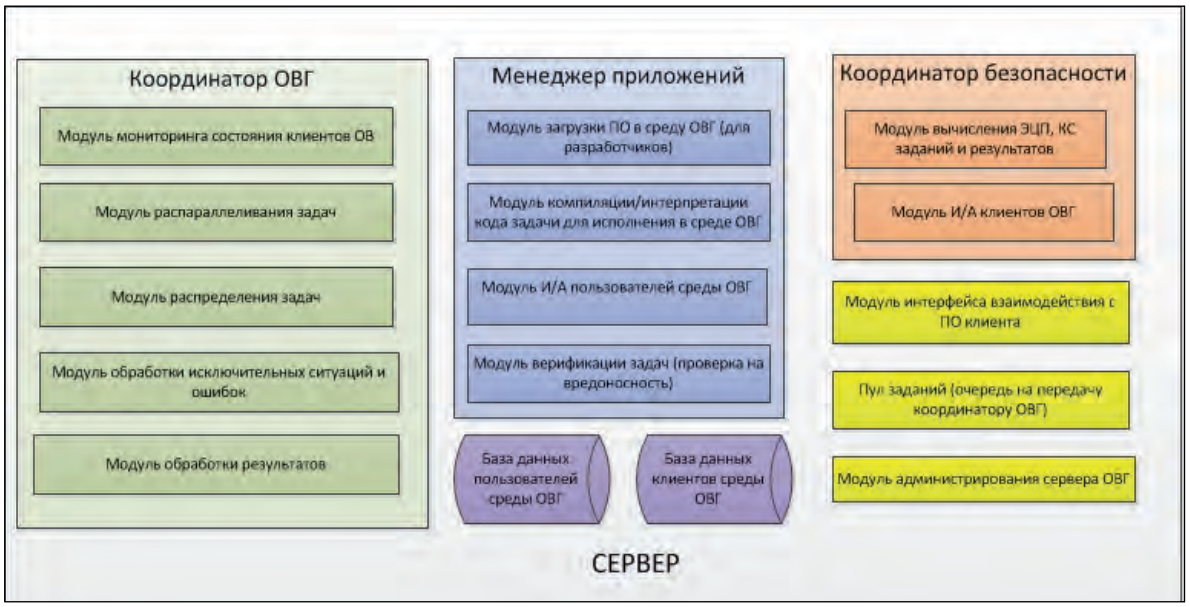

Рис. 1. Компоненты сервера среды ОВГ

Структура и алгоритм работы сервера среды ОВГ обеспечивают выполнение произвольных заданий, что невозможно для существующих реализаций Грид-сетей. Для этого разработан специальный модуль — «Модуль интерпретации/компиляции кода», который обеспечивает преобразование кода задания пользователя среды ОВГ в соответствии со спецификацией системы, в код, исполняемый на узлах Грид-сети. Сбалансированное распределение нагрузки на вычислительные узлы ГС обеспечивает «Модуль распределения задач», который формирует подоблако (подмножество узлов Грид-сети, программно-аппаратно удовлетворяющих требованиям к проведению вычислений конкретного задания) в соответствии с классификаций заданий, указанной в спецификации предлагаемого подхода.

Модель сервера среды ОВГ

На рис. 2 представлена модель сервера среды ОВГ.

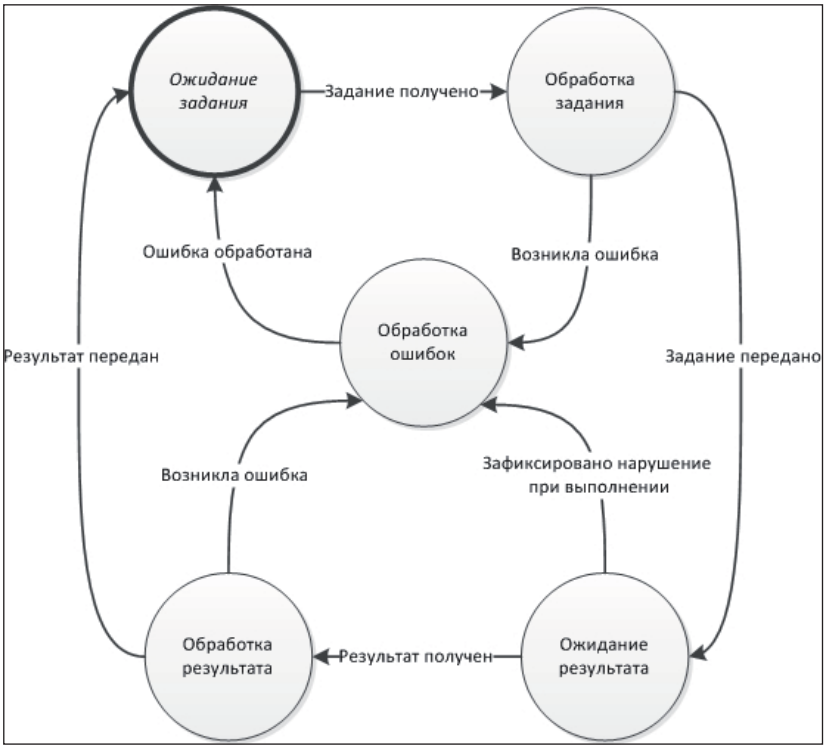

Рис. 2. Модель сервера среды ОВГ

Механизмы обеспечения безопасности сервера ОВГ

Процедура парольной аутентификации пользователя среды ОВГ и сервера ОВ происходит в момент обращения пользователя за услугами ОВ. В случае успешной аутентификации пользователь ОВГ может передать задание для выполнения. Иначе пользователь получает сообщение об ошибке аутентификации.

Верификация заданий перед их отправкой для вычисления на клиенты ОВ не позволяет передать небезопасный код для исполнения в Грид-сеть.

Далее рассмотрим модули, входящие в состав «Координатора безопасности», — модуль «Идентификация/аутентификация клиентов ОВ» и модуль «Создание и проверка ЭЦП».

Аутентификация производится на основе инфраструктуры открытых ключей, путем обмена сертификатами клиента ОВГ и сервера ОВГ. Корневым центром сертификации является самоподписанный центр сертификации, входящий в состав модуля «Идентификация/аутентификация клиентов ОВ». В случае неуспешной аутентификации считается, что ключи данного клиента скомпрометированы. Соответствующая пометка о ненадежности данного вычислительного узла делается в базе данных клиентов ОВ. Требуется переиздание сертификата для данного клиента ОВГ. В случае успешного прохождения процедуры аутентификации клиент ОВГ включается в состав подоблака для проведения вычислений.

Для обеспечения безопасной передачи кода задания и результата вычислений между «Координатором ОВГ» и клиентом ОВГ используется шифрование. Основными требованиями, предъявляющимися к способу шифрования, являются высокая скорость шифрования, безопасное распределение секретных ключей, отсутствие проблемы хранения секретных ключей клиентов ОВ.

Предъявленным требованиям удовлетворяет технология «Цифрового конверта». Эта технология заключается в генерации отправителем сеансового секретного ключа для зашифрования данных и зашифрования сеансового ключа на открытом ключе получателя.

Недостатком цифрового конверта является то, что получатель не знает, кто именно отправил ему сообщение, так как открытый ключ может быть доступен каждому. Для идентификации отправителя применяется ЭЦП. Использование ЭЦП гарантирует неотказуемость от авторства и целостность передаваемого сообщения [4]. За генерацию и проверку ЭЦП отвечает «Модуль создания и проверки ЭЦП», входящий в состав «Координатора безопасности».

Предложенный подход к развертыванию сред ОВ, реализованных на Грид-сетях, в качестве программно-аппаратной платформы обеспечивает возможность увеличения вычислительных ресурсов за счет включения все новых вычислительных узлов, представляющих собой средства вычислительной техники.

СПИСОК ЛИТЕРАТУРЫ:

1. *Mell P., Grance T.* The NIST Definition of Cloud Computing (Draft) // Recommendations of the National Institute of Standards and Technology. Special Publication 800-145 (Draft). 2011. P. 1–3.
2. Web как следующий шаг революции персональных компьютеров [Электронный ресурс]. URL: http://www.wdigest.ru/next.htm (дата обращения: 25.03.20012)..
3. Облачные технологии — 2009 [Электронный ресурс]. URL: http://www.ixbt.com/cm/cloud — computing.html (дата обращения: 28.04.20012).
4. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.