

Лекция 6. Введение в облачные вычисления

1. Основная идея облачных вычислений

Cloud computing (облачные вычисления) - это парадигма распределенных вычислений, где набор абстрактных, виртуализованных, динамически масштабируемых, дистанционно управляемых ресурсов и сервисов предоставляются по запросу удаленным пользователям через Интернет. Cloud computing не предполагает, что пользователь знает что-то об архитектуре и других особенностях вычислительных средств, которые он использует.

Основная идея cloud computing заключается в том, что клиент не должен создавать свой вычислительный центр (ВЦ) и обучать персонал инсталляции прикладных программ и обслуживанию системы. Следует также иметь в виду, ресурсы ВЦ оказываются недостаточными или избыточными. В обоих вариантах неизбежны дополнительные издержки. Кроме того, компания бывает вынуждена нанимать и обучать системных администраторов, специалистов по базам данных, управлению ИТ-ресурсами и сетевой безопасности. Если для крупной компании это может быть позволено, то для мелких и средних фирм это приводит к чрезмерным расходам. Cloud computing является откликом на быстро и динамически растущие потребности в вычислениях и разнообразных сервисах.

Инфраструктура cloud computing представляет собой систему предоставления вычислительных услуг информационными центрами, построенными на основе серверов. Такого рода сервисы стали возможны, когда уровень надежности и безопасности стал достаточно высок, а пропускная способность сетей сделала работу комфортной.

2. Типы облачных сервисов

Можно выделить 17 основных типов облачных сервисов, комбинация которых порождает новые типы сервисов:

- 1. Хранение данных в качестве услуги (storage-as-a-service) – предоставление по запросу нужного дискового пространства для конкретного приложения. Этот ресурс может располагаться удаленно;**
- 2. База данных в качестве услуги (database-as-a-service) – предоставление удаленного доступа к базам данных. Для пользователя это выглядит так, как если бы база данных была размещена локально;**
- 3. Информация в качестве услуги (information-as-a-service) – удаленный доступ к данным через интерфейс типа API. Это могут быть биржевые данные, кредитная информация, проверка адресов и идентификаций;**
- 4. Процесс в качестве услуги (process-as-a-service) – относится к провайдерам платформ, приложений и инфраструктуры;**
- 5. Приложение в качестве услуги (application-as-a-service, software-as-a-service) – представляет собой любую программу, доступ к которой предоставляется через web-интерфейс;**
- 6. Платформа в качестве услуги (platform-as-a-service) – комплексная услуга, включающая в себя разработку приложений, интерфейсов, баз данных, тестирование и т.д.;**
- 7. Интеграция в качестве услуги (integration-as-a-service) – включает в себя приложения, управление информационными потоками, прикладной дизайн;**
- 8. ИТ в качестве услуги (IT-as-a-service) – комплексная услуга, включающая в себя набор вышеперечисленных услуг;**
- 9. Аппаратная инфраструктура в качестве услуги (Hardware Infrastructure-as-a-service) – предоставление части сервера в качестве услуги. Клиенты могут использовать как весь сервер, так и его часть в рамках виртуальной машины;**
- 10. Программная инфраструктура в качестве услуги (Software Infrastructure-as-a-service) – набор прикладных программ, например, Microsoft Office, предоставляемых в качестве услуги;**

11. Безопасность в качестве услуги (security-as-a-service) – это предоставление через Интернет услуг безопасности. Хотя структура безопасности обычно строится локально, некоторые услуги реализуются удаленно, например, идентификация и сертификация, генерация, хранение и передача ключей доступа;

12. Управление в качестве услуги (management/governance-as-a-service) – сервис удаленного управления другими cloud-сервисами, сюда входит виртуализация, управление доступом, реализация определенных политик;

13. Тестирование в качестве услуги (testing-as-a-service) – предоставление возможности локального или удаленного тестирования различных видов сервисов, включая WEB-серверы;

14. Коммуникации в качестве услуги (SaaS) – предоставление каналов связи, например, высокоскоростных оптоволоконных, в качестве услуги;

15. Инфраструктура в качестве услуги (infrastructure-as-a-service) – фактически информационный центр в качестве сервиса. Пользователь получает доступ к определенному серверу (или серверам), его ОС и приложениям;

16. Восстановление после аварии в качестве услуги (Disaster Recovery-as-a-service) – услуга заключается в том, что в облаке хранится образ вашей системы и в случае аварии, система восстанавливается из удаленного образа;

17. Телевидение в качестве услуги (TV as-a-service) – подписка на телеканалы.

Для того чтобы выбрать нужный тип сервисов, пользователь должен выполнить следующие действия:

- 1. Составление списка платформ кандидатов вычислителей из облака;**
- 2. Пробная проверка платформ-кандидатов (проверка быстродействия, каналов связи);**
- 3. Выбор целевых платформ;**
- 4. Реализация целевых платформ.**

3. Категории облаков

В настоящее время выделяют три категории облаков: публичные, частные и гибридные.

Публичное облако – это ИТ-инфраструктура, используемая одновременно множеством компаний. Пользователи данных облаков не имеют возможности управлять ими и обслуживать их, вся ответственность по этим вопросам возложена на владельца данного облака. Абонентом предлагаемых сервисов может стать любая компания и индивидуальный пользователь. Они предлагают **легкий и доступный по цене способ развертывания web-сайтов или бизнес-систем, с большими возможностями масштабирования**, которые в других решениях были бы недоступны. Примеры: онлайн сервисы Amazon EC2 и Simple Storage Service (S3), Google Apps/Docs, Salesforce.com, Microsoft Office Web.

Частное облако – это безопасная ИТ-инфраструктура, контролируемая и эксплуатируемая в интересах одной-единственной организации. Организация может управлять частным облаком самостоятельно или поручить эту задачу внешнему подрядчику. Инфраструктура может размещаться либо в помещениях заказчика, либо у внешнего оператора, либо частично у заказчика и частично у оператора.

Гибридное облако – это ИТ-инфраструктура, использующая лучшие качества публичного и частного облаков, при решении поставленной задачи. Часто такой тип облаков используется, когда **организация имеет сезонные периоды активности, как только внутренняя ИТ-инфраструктура не справляется с текущими задачами, часть мощностей перебрасывается на публичное облако** (например, большие объемы статистической информации, которые в необработанном виде не представляют ценности для предприятия).

4. Преимущества и недостатки облачных вычислений

Достоинства облачных вычислений:

- **доступность** – облака доступны всем, из любой точки, где есть Интернет, с любого компьютера, где есть браузер. Это позволяет пользователям экономить на закупке высокопроизводительных компьютеров. Также сотрудники компаний становятся более мобильными так, как могут получить доступ к своему рабочему месту из любой точки земного шара, используя ноутбук, планшетник или смартфон. Нет необходимости в покупке лицензионного ПО, его настройки и обновлении, вы просто заходите на сервис и пользуетесь его услугами заплатив за фактическое использование;
- **низкая стоимость** – основные факторы снизившие стоимость использования облаков следующие: снижение расходов на обслуживание виртуальной инфраструктуры; оплата фактического использования ресурсов; развитие аппаратной части вычислительных систем, в связи с чем произошло снижение стоимости оборудования;
- **гибкость** – неограниченность вычислительных ресурсов (память, процессор, диски), за счет использования систем виртуализации, процесс масштабирования и администрирования облаков становится достаточно легкой задачей;
- **надежность облаков**, особенно находящихся в специально оборудованных центрах обработки данных (ЦОД), очень высокая так, как такие ЦОД имеют всю необходимую инфраструктуру (резервные источники питания, охрану, профессиональных работников, регулярное резервирование данных, высокую пропускную способность Интернет канала, устойчивость к DDOS атакам);
- **безопасность** – облачные сервисы имеют высокий уровень безопасности (при должном ее обеспечении).

К недостаткам cloud computing можно отнести следующие:

- **постоянное соединение с сетью** – для получения доступа к услугам облака необходимо постоянное соединение с сетью Интернет. Однако в наше время это не такой и большой недостаток, особенно с приходом технологий сотовой связи 3G и 4G;
- **программное обеспечение и его кастомизация** – есть ограничения ПО, которое можно разворачивать на облаках и предоставлять его пользователю;
- **конфиденциальность данных**, хранимых на публичных облаках в настоящее время вызывает много споров, но в большинстве случаев эксперты сходятся в том, что не рекомендуется хранить наиболее ценные для компании документы на публичном облаке, так как в настоящее время нет технологии которая бы гарантировала 100% конфиденциальность хранимых данных;
- **надежность хранимой информации** – если вы потеряли информацию, хранимую в облаке, то вы ее потеряли навсегда.

5. Архитектура облачных вычислений

Архитектура облачных вычислений содержит пять главных действующих субъектов (actors). Каждый субъект выступает в роли (role) и выполняет действия (activities) и функции (functions).

Субъект	Определение
Облачный потребитель	Лицо или организация, использующая услуги облачных провайдеров
Облачный провайдер	Лицо, организация или сущность, отвечающая за доступность облачной услуги для облачных потребителей
Облачный аудитор	Участник, который может выполнять независимую оценку облачных услуг, обслуживания информационных систем, производительности и безопасности реализации облака
Облачный брокер	Сущность, управляющая использованием, производительностью и предоставлением облачных услуг, а также устанавливающая отношения между облачными провайдерами и облачными потребителями
Облачный оператор связи	Посредник, предоставляющий услуги подключения и доставки облачных услуг от облачных провайдеров к облачным потребителям

Среди представленных пяти субъектов, **облачный брокер опционален**, т.к. облачные потребители могут получать услуги напрямую от облачного провайдера.

Приведем пример нескольких сценариев взаимодействия субъектов.

Сценарий 1: Облачный потребитель может запросить услугу (сервис) у облачного брокера вместо прямого контактирования с облачным провайдером (рис. 1). Облачный брокер может создать новый сервис, комбинируя набор сервисов или расширяя существующий сервис. В этом примере облачный провайдер невидим облачному потребителю.



Рисунок 1 – Взаимодействие облачного потребителя с провайдером посредством брокера

Сценарий 2: Облачный оператор связи предоставляет услуги подключения и доставку облачных услуг от облачного провайдера облачному потребителю. Облачный провайдер устанавливает соглашение об уровне обслуживания SLA (Service Level Agreement) с облачным оператором и может запрашивать выделенные и защищенные соединения.

Сценарий 3: Облачный аудитор проводит независимую оценку обслуживания и безопасности реализации облачной услуги (рис. 2).



Рисунок 2 – Участие облачного аудитора

6. Безопасность cloud computing

Все виды cloud computing предполагают передачу данных провайдеру услуг. Это безусловно создает дополнительные уязвимости, ведь критическая информация оказывается вне зоны контроля ее владельца. Но даже когда такие данные находятся на сервере владельца, они не полностью защищены. Дело здесь не только во внешних хакерах. **Наибольшую опасность представляют сотрудники самой организации-владельца, имеющие доступ в том числе и к критической информации.** Вероятность несанкционированного прочтения, после того как информация попала к провайдеру услуг, минимальна. Но при передаче следует помнить о **возможности атаки "человек-по-середине"**, когда могут подменяться общедоступные ключи. По этой причине **многоуровневое использование сертификатов является обязательным.**

При заключении договора нужно оговаривать определенное значение коэффициента доступности сервиса (uptime), а также время восстановления системы после отказа.

В случае cloud computing **обеспечение безопасности и защиты сетей следует переместить в сферу безопасности услуг и приложений.** Традиционные ранее **политики безопасности (DMZ и защита периметра)** здесь **перестают работать.** Нюансы возникают из-за того, что на общем сервере провайдера услуг могут находиться данные и программы разных клиентов. Здесь оказывается особенно важно правильно выбрать провайдера, это особенно важно с точки зрения внешних физических аспектов безопасности. Далее **нужно определить, что следует хранить и использовать локально, а что перенести в облако.** Если все элементы системы безопасности будут выполнены правильно, безопасность при переходе в "облако" увеличится.

Вопросы

1. В чем отличие cloud от GRID?
2. Приведите хотя бы пять типов облачных сервисов.
3. Какие категории облаков применяются в настоящее время?
4. Назовите преимущества и недостатки облачных вычислений.
5. Назовите субъектов облачных вычислений и их роли.
6. Каковы проблемы безопасности облачных вычислений и пути их решения?
7. Приведите примеры наиболее известных облачных сервисов.