ПОДХОДЫ К ПОВЫШЕНИЮ КАЧЕСТВА ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ И СЕРВИСОВ МУЛЬТИОБЛАЧНЫХ ПЛАТФОРМ НА БАЗЕ ТЕХНОЛОГИЙ VNF И SDN

Парфёнов Д.И., Болодурина И.П.
Оренбургский государственный университет, г. Оренбург

В настоящее время крупные коммерческие и государственные организаций, в том числе промышленные предприятия (в областях электроэнергетики, машиностроения, добычи и переработки полезных ископаемых, систем жизнеобеспечения и т.п.) переносят свою информационную инфраструктуру из физических центров обработки данных (ЦОД) в виртуальные. Такая оптимизация позволяет существенно экономить средства для организаций, а так же развивать рынок предоставления услуг в сфере аренды центров обработки данных [1-2].

На сегодняшний день не так много компаний способных предоставлять услугу виртуального ЦОД (Virtual Data center as a service, VDCaaS) своим клиентам. Такое положение связано с тем, что требования клиентов к услуге VDCaaS существенно отличается от предоставления услуг IaaS (инфраструктура, как услуга) и даже DCaaS (ЦОД, как услуга). Множество требований касается вопросов безопасности функционирования систем. Так, например, в виртуальном ЦОД предприятия размещают критически важные сервисы и приложения, от которых напрямую зависит их экономическая безопасность при осуществлении обработки финансовых потоков или безопасность людей [3-4]. Такие объекты инфраструктуры в первую очередь становятся целью кибератак.

Другой проблемой предоставления услуг виртуального ЦОД является задача построения комплексной виртуальной инфраструктуры на базе существующих физических сетевых и вычислительных ресурсов с предоставлением полноценного доступа клиента к управлению всеми функциональными возможностями реального ЦОД. Критической точкой любой инфраструктуры физического ЦОД с течением времени становится разнородность используемого оборудования. Лидеры мирового рынка сетевого оборудования компании Cisco Systems, Huawei, Juniper, HP и др. навязывают использование собственных средств мониторинга и управления сетевыми устройствами и протоколами, что не позволяет гибко и оперативно подстраивать инфраструктуру под текущие задачи клиента. Кроме того высокая стоимость такого оборудования, несмотря на гарантию надежности, накладывает существенные ограничения на масштабируемость и резервирование, закладываемые в физическую инфраструктуру ЦОД. Это в дальнейшем может приводить к долговременным простоям, связанным с заменой, вышедших из строя объектов, или модернизацией узлов для расширения функциональных возможностей [5-6].

Как отмечалось ранее, одним из требований клиентов, предъявляемых к предоставлению услуги виртуального ЦОД, является доступ к полноценным средствам управления сетевой инфраструктурой, включая различные сервисы сетевой безопасности и обеспечения качества обслуживания. Использование традиционных подходов к организации сетевой инфраструктуры не позволяет это реализовать для множества клиентов в пределах одного ЦОД без построения выделенной физической сети, что приводит к существенным бюджетным ограничениям [7]. В последнее время для решения данной проблемы применяется технология программно-конфигурируемых сетей (Software-Defined Networks, SDN), которая позволяет отделить (абстрагировать) уровень управления сетью (control plane) от нижележащего уровня пересылки пакетов (data plane) за счет передачи функций управления (маршрутизаторами, коммутаторами и т.д.) в приложения, работающие на выделенных вычислительных узлах (контроллерах). Планирование сети и управление трафиком при этом происходит программным путем. Для приложений верхнего уровня предоставляются интерфейсы прикладного программирования API. Таким образом, ввод новых услуг на сети ускоряется и облегчается.

На практике подход, применяемый в программно-конфигурируемых сетях, позволяет повысить эффективность, безопасность и надежность передачи данных за счет гибкого реконфигурирования маршрутов и настройки политик доступа к ресурсам на уровне потоков данных. Кроме того технология программно-конфигурируемых сетей позволяет пользователям создавать новые сервисы и загружать их в сетевое оборудование. Однако клиентам виртуальных ЦОД требуется не только традиционные сетевые функции управления трафиком, но и специализированные программные или аппаратные решения, обеспечивающие высокую производительность для конкретных задач, например анализ и фильтрация сетевых пакетов (Deep packet inspection, DPI), межсетевой экран (Firewall) и другие. В традиционных сетях для таких целей применяют специализированные устройства, отвечающие должному классу по производительности и функционалу. В концепции услуги виртуальных ЦОД, доступ к управлению физическими устройствами может быть ограничен, и они чаще всего обеспечивают внешний периметр безопасности инфраструктуры ЦОД.

Для решения этой проблемы разработана технология виртуализации функций сетевых элементов телекоммуникационной сети (Network Functions Virtualization, NFV), позволяющая использовать программные модули, работающие на стандартных вычислительных узлах и виртуальных машинах (VM) вместо специализированных устройств. Эти программные модули могут взаимодействовать между собой для предоставления услуг связи, чем ранее занимались аппаратные платформы. Технологии SDN и NFV являются независимыми компонентами инфраструктуры виртуального ЦОД, дополняющие друг друга. Однако в рамках концепции обеспечения безопасности и качества обслуживания для приложений и сервисов

мультиоблачных платформ требуется комплексный подход, обеспечивающий полноценное управление всей сетевой инфраструктурой виртуального ЦОД.

В рамках исследования предложено решение в котором все задачи связанные с управлением ресурсами виртуального ЦОД будут подвергаться проактивному прогнозированию и работать автоматизировано, основываясь на принципах самоорганизации в части размещения объектов виртуальной инфраструктуры, на физических узлах и устройствах, а так же в части распределения потоков данных для обеспечения надежности мультиоблачной платформы.

Достигнуть поставленной цели возможно путем разработки эффективных алгоритмических и программных решений, а так же построения моделей обеспечения безопасности и качества обслуживания для приложений и сервисов мультиоблачной платформы, расположенной на базе инфраструктуры виртуального ЦОД.

Определим эффективность управления объектами инфраструктуры для обеспечения безопасности и качества обслуживания, как способность распределять и балансировать нагрузку между устройствами, максимизируя при этом количество обрабатываемых запросов и минимизируя возможность отказа в обслуживании при возникновения целенаправленных или непреднамеренных действий третьих лиц, направленных на выведение из строя отдельных компонентов или всей мультиоблачной платформы в целом.

Использование концепции мультиоблачных платформ позволяет одновременно размещать в пределах одного виртуального ЦОД частные, публичные и гибридные облачные системы с поддержкой контейнеризации сервисов и приложений на базе Docker, работающие под управлением различных оркестраторов OpenStack, OpenNebula, CloudStack и др. В основе подхода программно-конфигурируемых сетей лежит возможность динамически управлять пересылкой данных в сети с помощью открытого протокола OpenFlow. Все сетевые коммутаторы, поддерживающие OpenFlow, объединяются под управлением контроллера OpenFlow, который обеспечивает приложениям доступ к управлению сетью. Каждый коммутатор OpenFlow имеет таблицу потоков, содержащую правила обработки пакетов. Каждое правило включает две части – признаки заголовков пакетов и набор действий. При поступлении в коммутатор нового пакета, происходит сопоставление его заголовков с признаками правил в таблице. В случае совпадения выполняются все действия из соответствующего набора. Если подходящее правило в таблице отсутствует, то пакет передается контроллеру OpenFlow. Контроллер принимает решение о дальнейших действиях над пакетом, которое реализуется в виде команды передачи пакета на определенный порт коммутатора и/или в установке для пакета нового правила в таблицу данного и, возможно, других коммутаторов. Признаки заголовков позволяют управлять пакетами на уровнях L1–L3 модели OSI.

Таки образом за счет применения виртуализации сетевых компонентов и внедрения эффективных алгоритмов управления виртуальными ресурсами

возможно повышение производительности их работы на 30-40% по сравнению с аналогичными компонентами традиционной инфраструктуры телекоммуникационных сетей. Так же это позволит сократить время простоя на модернизацию сетевых и вычислительных узлов, а также снизит на 50-60% затраты на закупку нового дорогостоящего оборудования, поддерживающего ранее недоступный функционал, для возможности предоставления новых сервисов и услуг для клиентов в короткие сроки.

Работа выполнена при поддержке РФФИ (научные проекты 16-37-60086 мол_а_дк и 16-07-01004), Президента Российской Федерации, грант для государственной поддержки молодых российских ученых – кандидатов наук (МК-1624.2017.9).

Список литературы

1. Болодурина И.П., Парфёнов Д.И. Алгоритмы комплексной оптимизации потребления вычислительных ресурсов в облачной системе дистанционного обучения [Текст] / И.П. Болодурина, Д.И. Парфёнов // Вестник Оренбургского государственного университета. – 2013. - № 9. – С. 177-184.

2. Болодурина И.П., Парфёнов Д.И. Управление потоками данных в высоконагруженных информационных системах, построенных на базе облачных вычислений [Текст] / И.П. Болодурина, Д.И. Парфёнов // Системы управления и информационные технологии. – 2015. - № 1.1. – С. 111-118.

3. Bocchi E., Drago I., Mellia M. Personal Cloud Storage Benchmarks and Comparison // IEEE Transactions on Cloud Computing. 2015. Vol. 99. – IEEE, 2015. – pp. 1-14

4. Bolodurina I., Parfenov D., Shukhman A. Approach to the effective controlling cloud computing resources in data centers for providing multimedia services //Control and Communications (SIBCON), 2015 International Siberian Conference on. – IEEE, 2015. – pp. 1-6.

5. Charuenporn P., Intakosum S. Qos-Security Metrics Based on ITIL and COBIT Standard for Measurement Web Services //J. UCS. – 2012. – Vol. 18. – No. 6. – pp. 775-797, available at: www. http://jucs.org/jucs_18_6/

6. Rajiv R., Benatallah B., Schahram D., Michael P. Cloud Resource Orchestration Programming: Overview, Issues, and Directions // IEEE Internet Computing. 2015. Vol. 19, Issue: 5. – pp. 46-56.

7. Thiago A. L., Genez L. F., Bittencourt E., Madeira R. M. Workflow scheduling for SaaS / PaaS cloud providers considering two SLA levels // Network Operations and Management Symposium (NOMS).– IEEE, 2012. – pp. 906-912.