

УДК 004.75

doi: 10.17586/2226-1494-2019-19-5-931-938

СИСТЕМА УПРАВЛЕНИЯ МАСШТАБИРУЕМЫМ ГЕОГРАФИЧЕСКИ РАСПРЕДЕЛЕННЫМ ЦЕНТРОМ ОБРАБОТКИ ДАННЫХ

С.Э. Хоружников^a, А.Е. Шевель^{a,b}

^a Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

^b НИЦ «Курчатовский Институт» – ПИЯФ, Гатчина, ЛО, 188300, Российская Федерация

Адрес для переписки: xse@itmo.ru

Информация о статье

Поступила в редакцию 16.07.19, принята к печати 25.08.19

Язык статьи — русский

Ссылка для цитирования: Хоружников С.Э., Шевель А.Е. Система управления масштабируемым географически распределенным центром обработки данных // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 5. С. 931–938. doi: 10.17586/2226-1494-2019-19-5-931-938

Аннотация

Предмет исследования. Представлены результаты разработки системы управления масштабируемым географически распределенным центром обработки и хранения данных. Особое внимание уделено гибкости перестройки системы на новые задачи эффективности использования ресурсов, надежности функционирования в условиях отказов компонентов системы и защите информации от несанкционированного доступа. **Метод.** Использован подход, основанный на технологиях программно-конфигурируемых инфраструктур. Технические решения созданных программных компонент реализованы на базе свободно распространяемого программного обеспечения. Для защиты линий связи между локальными центрами обработки данных в составе масштабируемого географически распределенного центра обработки и хранения данных применены технологии квантовой коммуникации на боковых частотах. Компоненты разработанной системы интегрированного управления реализованы в форме программных агентов, выполняющихся в операционно-изолированной среде. **Основные результаты.** Создан аппаратно-программный комплекс, функционирующий по модели «Инфраструктура как услуга». Экспериментальные исследования системы интегрированного управления проведены на макете масштабируемого географически распределенного центра обработки и хранения данных, построенного совместно с компанией АО «СМАРТС» (г. Самара). Эти исследования показали работоспособность и высокую эффективность примененных решений для удовлетворения технических требований к разработке. **Практическая значимость.** Рассмотренный аппаратно-программный комплекс может быть использован при формировании или модификации масштабируемого географически распределенного центра обработки и хранения данных в первую очередь государственными организациями, поскольку является отечественной разработкой, в которой отсутствует заимствованное проприетарное программное обеспечение. Компоненты системы могут быть применены и при построении частной облачной инфраструктуры.

Ключевые слова

программно-конфигурируемые сети, виртуализация сетевых функций, центр обработки данных, программный агент, квантовая система распределения ключей, программно-конфигурируемое хранилище данных, OpenStack, Сeph

Благодарности

Разработка выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации (договор № 03.G25.31.0229).

doi: 10.17586/2226-1494-2019-19-5-931-938

MANAGEMENT SYSTEM FOR SCALABLE GEOGRAPHICALLY DISTRIBUTED DATA CENTER

S.E. Khoruzhnikov^a, A.Ye. Shevel^{a,b}

^a ITMO University, Saint Petersburg, 197101, Russian Federation

^b Petersburg Nuclear Physics Institute named by B.P. Konstantinov of National Research Centre «Kurchatov Institute» (NRC «Kurchatov Institute» — PNPI), Gatchina, Leningrad District, 188300, Russian Federation

Corresponding author: xse@itmo.ru

Article info

Received 16.07.19, accepted 25.08.19

Article in Russian

For citation: Khoruzhnikov S.E., Shevel A.Ye. Management system for scalable geographically distributed data center. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 5, pp. 931–938 (in Russian). doi: 10.17586/2226-1494-2019-19-5-931-938

Abstract

Subject of Research. The paper presents results of the management system development for a scalable geographically distributed data center. Special attention is paid to system versatility in view of new tasks, resource efficiency, operational reliability in the conditions of system component failures, and information access security. **Method.** An approach based on technologies of software-configured infrastructures was used. The technical solutions of the created software components were implemented on the basis of free and open source software. Quantum communication technologies at the side frequencies were used for protection of the data links between the local data processing centers as part of a scalable geographically distributed data center. The components of the developed integrated management system were implemented in the form of software agents running in an operating-isolated environment. **Main Results.** The hardware-software complex has been created, functioning according to the “Infrastructure as a Service” model. Experimental studies of the integrated management system were carried out on a prototype of a scalable geographically distributed data center built together with the SMARTS Ltd company (the city of Samara). These studies have shown the feasibility and high efficiency of the designed solutions meeting the technical requirements for the development. **Practical Relevance.** The considered hardware-software complex can be used in the formation or modification of a scalable geographically distributed data center primarily by government organizations, since it is an indigenous Russian technology without applying borrowed proprietary software. The system components can be used in the development of private cloud infrastructure.

Keywords

software-configured networks, Network Functions Virtualization, data center, program agent, quantum key distribution, software-configured storage, OpenStack, Ceph

Acknowledgments

The research has been carried out with the financial support of the Ministry of Science and Higher Education of the Russian Federation under grant agreement No.03.G25.31.0229.

Введение

В настоящее время с целью обеспечения эффективного использования вычислительных ресурсов отдельных центров обработки и хранения данных (ЦОД) реализуется подход на основе их объединения, например, объединение ЦОД типа Grid computing (Грид компьютеринг) и Cloud computing (облачный компьютеринг), таким образом, выполняется требование на гибкость перераспределения имеющихся мощностей. Одним из примеров может служить крупнейшая система типа Грид — это WorldLHC Computing Grid [1], которая применяется для обработки экспериментальных данных в фундаментальных исследованиях свойств материи. Другими примерами являются известные облачные системы Amazon¹, Google², Azure³, Yandex⁴, которые обслуживают большое число потребителей. Например, Azure имеет около пятисот миллионов зарегистрированных пользователей.

Большое значение имеет географическое распределение ЦОДов [2], которое позволяет избежать остановки сервисов или даже безвозвратной потери данных во время технологических аварий, природных катастроф (наводнения, землетрясения, ураганы, удары молнии, цунами и т.д.) и социальных инцидентов: (теракты, гражданские беспорядки и пр.).

Отметим разницу подходов к объединению ЦОД: Грид и облачные системы. Подход типа Грид позволяет выполнить довольно специфическое объединение ресурсов существующих ЦОД, которые принадлежат разным юридическим организациям, нуждающимся в некоторых общих результатах обработки данных, представляющих общий интерес для участников. Хорошим примером являются научные системы типа Грид, когда несколько университетов и/или исследовательских центров объединяют свои вычислительные мощности на некоторое время для решения общей для всех участников задачи.

В облачной системе, построенной на принципе «Инфраструктура как сервис» (Infrastructure as a Service – IaaS), имеется возможность реализовать любые архитектуры в том числе и Грид, т.е. IaaS является более общим решением в сравнении с архитектурой Грид.

На основе рассмотренных выше примеров существующих публичных систем можно сформулировать основные требования к географически распределенной IaaS:

- относительная простота перераспределения ресурсов между локальными ЦОД (вычислительная мощность, хранилища данных, каналы передачи), географически удаленных друг от друга;
- относительная простота перераспределения ресурсов между локальными ЦОД (вычислительная мощность, хранилища данных, каналы передачи), географически удаленных друг от друга;

¹ Amazon EC2 — Режим доступа: // <https://aws.amazon.com/ru/ec2/>, свободный. Яз. англ. (дата обращения 06.02.2019).

² Google Cloud — Режим доступа: // <https://cloud.google.com/>, свободный. Яз. англ. (дата обращения 07.03.2019).

³ Microsoft Azure — Режим доступа: // <https://azure.microsoft.com/>, свободный. Яз. англ. (дата обращения 07.03.2019).

⁴ Яндекс Облако — Режим доступа: // <https://cloud.yandex.ru/>, свободный. Яз. англ. (дата обращения 07.03.2019).

— безопасность/надежность передачи и долговременного хранения данных;
— постепенная (стадийная) деградация при выходе из строя аппаратных и/или программных компонент. Выходы из строя отдельных компонентов не должны приводить к остановке системы в целом.

Дополнительной важной задачей является объединение «темных» ЦОДов (dark data center) [3], которые имеют ряд преимуществ в сравнении с традиционными ЦОДами, например, отсутствие на ЦОДе постоянного обслуживающего персонала. Такой ЦОД функционирует закрытым на ключ. Обслуживающий персонал прибывает в расположение ЦОДа только в случае чрезвычайных ситуаций.

Анализ публикаций, посвященных архитектурно-техническим решениям, которые используются при создании систем управления распределенной компьютерной инфраструктурой, например [4], показывает, что наиболее перспективными из них для создания системы интегрированного управления (СИУ) масштабируемым географически распределенным ЦОД (МГРЦ) являются:

- операционная платформа: Линукс;
- программно-конфигурируемые сети (ПКС) — Software Defined Network (SDN) и Виртуализация Сетевых Функций (ВСФ) — Network Functions Virtualization (NFV) [5];
- программно-конфигурируемое хранилище данных (ПКХД) — Software Defined Storage (SDS) [6, 7];
- инфраструктура как код (ИК) — Infrastructure as Code (IC) [8];
- реализации систем в виде программных агентов [3];
- квантовая технология распространения ключей кодирования данных [9].

Выбор ниже приведенных технических решений определялся несколькими соображениями: современность, активность разработчиков компонентов и деловые контакты с ними, опыт использования в реальных проектах:

- операционная система (ОС): Naulinux.ru (клон RHEL¹);
- программный контроллер ПКС: Ryu²;
- хранение данных: на данном этапе проекта выбрана CEPH.com [10];
- операционная платформа для управления виртуальными объектами, а также вэб-порталов: Openstack.org;
- система управления конфигурациями и удаленного выполнения операций: SaltStack.org;
- мониторингирование физических и виртуальных ресурсов: Zabbix.org;
- визуализация: Kibana³, Grafana⁴.

Перечисленные компоненты рассматриваются как полуфабрикаты, которые могут помочь реализовать те или иные подходы к проектированию всей системы. Среди прочего важным является поддержание определенной независимости СИУ от конкретных продуктов. Для создания предпосылок независимости при проектировании системы управления МГРЦ использованы следующие подходы:

- архитектурное решение должно быть выполнено на базе технологий программно-конфигурируемых инфраструктур;
- программные компоненты системы должны быть реализованы с использованием только свободного распространяемого программного обеспечения, которое настраивается путем конфигурирования под конкретный функционал;
- компоненты системы должны быть созданы как программные агенты, которые выполняются в операционно-изолированной среде в форме виртуальных машин или контейнеров;
- для защиты линий связи между ЦОДами должна быть применена технология квантовой коммуникации на боковых частотах.

Архитектура программной части системы интегрированного управления масштабируемого географически распределенного центра обработки и хранения данных

На основе принятых подходов создана Система Интегрированного Управления (СИУ) МГРЦ, архитектура которой представлена на рис. 1.

Отметим, что СИУ построена на основе программных агентов, каждый из которых выполняется в операционно-изолированной среде в форме виртуальных машин (ВМ) или контейнеров.

¹ Red Hat Enterprise Linux – Режим доступа: // <https://www.redhat.com/en/technologies/linux-platforms/enterprise-linux>, свободный. Яз. англ. (дата обращения 07.03.2019).

² Build SDN Agilely — Режим доступа: // <https://osrg.github.io/ryu/>, свободный. Яз. англ. (дата обращения 07.03.2019).

³ Kibana — Режим доступа: // <https://www.elastic.co/products/kibana>, свободный. Яз. англ. (дата обращения 07.03.2019).

⁴ Grafana — Режим доступа: // <https://grafana.com/>, свободный. Яз. англ. (дата обращения 07.03.2019).

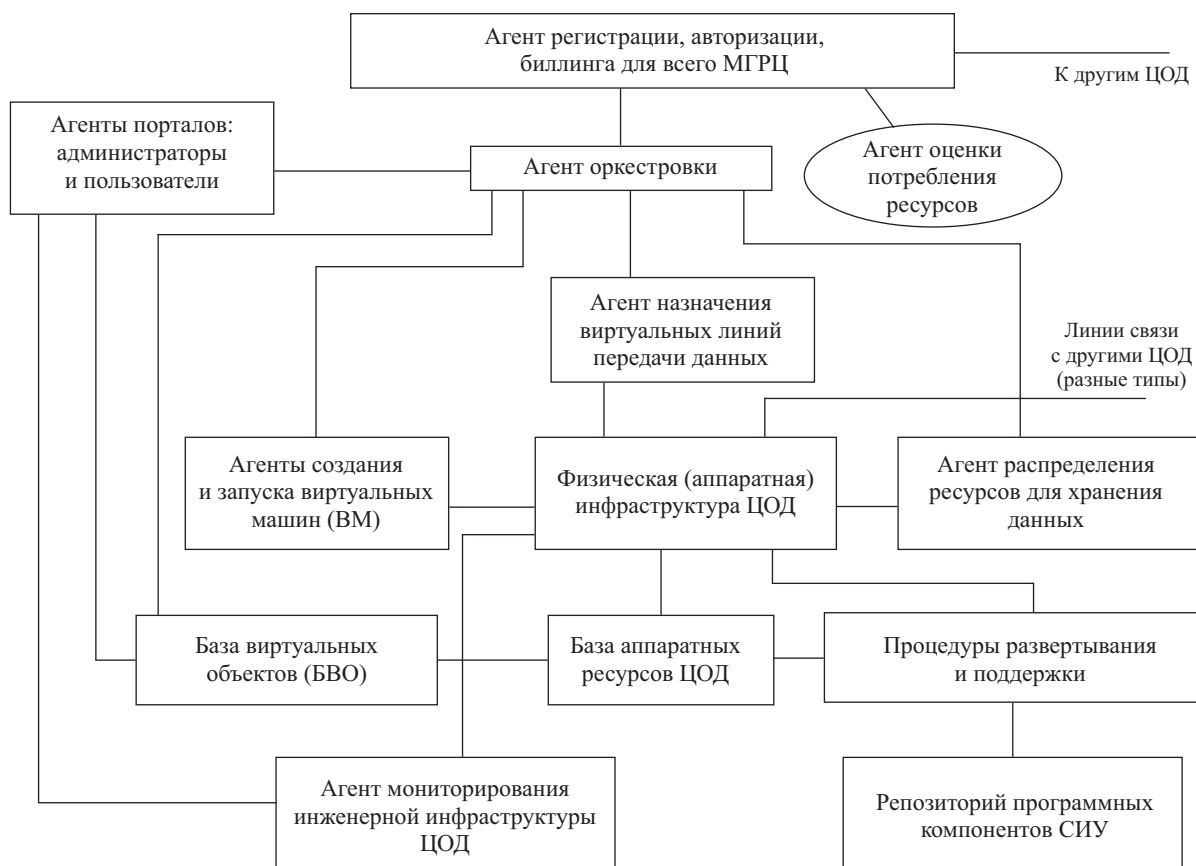


Рис. 1. Архитектура программной системы интегрированного управления масштабируемого географически распределенного центра обработки и хранения данных для одного локального центра обработки и хранения данных

Взаимодействие между программными агентами реализовано посредством специально разработанного протокола, который включает в себя организацию очередей запросов с использованием распределенной системы управления очередями сообщений RabbitMQ между агентами и сохранение всех запросов в базе данных, которая подошла по соображениям упомянутым выше.

Важным элементом системы, объединяющим все ЦОДы в составе МГРЦ, является каталог РЕГИСТРИ, внутри которого имеются подкаталоги, описывающие каждый отдельный ЦОД, а также линии передачи данных между ЦОДами. Каталог РЕГИСТРИ автоматически реплицируется на все ЦОДы в составе МГРЦ. Доступ к данным в каталоге РЕГИСТРИ осуществляется по https, сами данные в каталоге хранятся в закодированном виде. Таким образом, доступ к данным в каталоге РЕГИСТРИ возможен только авторизованным программным агентам.

Все программные агенты МГРЦ запускаются автоматически в процессе загрузки аппаратных серверов МГРЦ. Каждый программный агент использует конфигурационные параметры из каталога РЕГИСТРИ. Поскольку изменение архитектуры и/или состава МГРЦ отражается в РЕГИСТРИ, то не требуется никаких изменений в программных агентах.

Ниже приведено описание основных функций, входящих в состав СИУ агентов.

Агент регистрации, авторизации и биллинга является управляющим агентом для всего МГРЦ. Он предназначен для регистрации клиентов (пользователей), выполнения функций биллинга, функций аутентификации и авторизации, выдаёт распоряжения о перераспределении ресурсов (вычислительной мощности, линий передачи данных, хранилищ данных) в соответствии с запросами клиентов. Только этот агент выдаёт распоряжения о любом изменении конфигурации МГРЦ. На портале агента после регистрации пользователь сможет запросить ресурсы из публичного облака (виртуальные машины, виртуальные хранилища данных (ВХД), виртуальные линии передачи данных) для выполнения задач пользователя. Запросы на выделение ресурсов направляются для реализации в агент оркестровки. Пользователь может запросить создание частного облака, в котором администратор может выделять ресурсы в рамках квот частного облака пользователям частного облака. Детальное описание функционала этого агента в отношении биллинга выходит за пределы данной статьи.

Часть программных агентов имеют порталы для взаимодействия с потребителями. Например, портал администраторов и пользователей предназначен для интерактивного взаимодействия администраторов и пользователей с СИУ. Он обеспечивает следующий функционал:

— для пользователей публичного облака: просмотр состояния подписки пользователя в публичном облаке;

— для администраторов частного облака: выделение/перераспределение ресурсов конкретному пользователю в частном облаке;

— портал предоставляет администраторам возможности подготовки и редактирования шаблонов (текстовых файлов) на выполнение запросов к другим агентам.

Аналитический портал предоставляет администратору средства визуализации протекающих процессов в МГРЦ и в каждом локальном ЦОДе в составе МГРЦ. Функционал агента реализован с использованием программных продуктов Grafana и Kibana.

Портал конфигурации услуг предоставляет информацию об услугах, которые пользователь может запросить на портале Агент регистрации, авторизации и биллинга.

Агент оркестровки получает от Агента регистрации, авторизации и биллинга запросы на конфигурирование виртуальных ресурсов МГРЦ. Анализируется формат запроса и уточняется физическая реализуемость запроса. В случаях неверного формата и/или других ошибок в Агент регистрации, авторизации и биллинга возвращается ответ с описанием ошибки. Если запрос оказался корректным, то он отправляется для дальнейшей реализации в один из исполнительных агентов: агент создания и запуска виртуальных машин, агент распределения ресурсов для хранения данных, агент назначения виртуальных линий передачи данных.

После успешного создания запрошенного виртуального объекта все данные о созданном объекте записываются в Базу Виртуальных Объектов.

Агент оркестровки может принимать от Агента регистрации, авторизации и биллинга транзакции, состоящие из нескольких запросов. При выполнении транзакции этот агент следует правилу «все или ничего», т.е. если хоть один запрос из транзакции выполнен неуспешно, то отменяются все остальные запросы, даже если они выполнены успешно.

Агент оркестровки может получать сигналы о чрезвычайных ситуациях от других агентов, например, от Агента мониторинга инженерной инфраструктуры. Если получено сообщение о чрезвычайной ситуации, то включается процедура оценки ущерба, которая определяет, в чем конкретно выражается ущерб для клиентов и что может предпринять администратор МГРЦ для минимизации ущерба.

Агент создания и запуска виртуальных машин реализует процедуру создания и запуска ВМ. Процедура реализуется средствами OpenStack. Если создание и запуск ВМ выполнено успешно, то он сообщает об этом Агенту оркестровки, который создает запись в Базе Виртуальных Объектов.

Если создание или запуск ВМ не удалось выполнить, то причины неуспешной операции передаются Агенту оркестровки, который при этом не создает никаких записей в Базе Виртуальных Объектов, а только информирует Агента регистрации, авторизации и биллинга о причинах неуспешного выполнения запроса.

Агент распределения ресурсов для хранения данных получает запросы на создание ВХД от Агента оркестровки и выполняет создание кластера хранения данных средствами CEPH. Процесс создания кластера хранения данных реализуется средствами конфигурирования Saltstack, который формирует необходимое число ВМ для демонов CEPH: OSD, MGR, MON.

Созданный кластер CEPH служит в качестве виртуального хранилища данных. ВХД может иметь несколько типов, которые отличаются по организации доступа: блочный, файловый, объектный.

Запрос на создание ВХД может сопровождаться описанием требуемых свойств ВХД, которые в данном проекте именуется как Требования по Качеству Обслуживания (ТКО). Среди значений ТКО могут быть возможности кодирования данных, число реплик данных и другие.

Агент назначения виртуальных линий передачи данных формирует виртуальную линию передачи данных для обмена данными между указанными ВМ. Создание виртуальной линии связи формируется посредством управляющих команд, поступающих от рассматриваемого агента в контроллер ПКС (Ryu), который в свою очередь загружает необходимую маршрутизацию в программные сетевые коммутаторы (OpenVswitch).

Среди ТКО для виртуальных линий передачи данных имеются требования на кодирование передаваемых данных, в том числе требование на использование квантового распределения ключей кодирования, которое в настоящей работе реализовано на базе технологии квантовых коммуникаций на боковых частотах модулированного излучения. Выбор этой технологии обусловлен высокими эксплуатационными характеристиками, превосходящими аналоги [11]. Физические принципы ее функционирования изложены в работе [9], а схема ее реализации в действующей телекоммуникационной сети представлена в [11] с экспериментальным подтверждением надежности и долговременной стабильности предложенного решения.

Агент мониторинга инженерной инфраструктуры контролирует состояние всех элементов, входящих в ее состав: электропитание, системы контроля климата и пожаротушения, датчики проникновения в помещении ЦОДа, видекамеры для видеонаблюдения и др. Он функционирует по большей части независимо и не участвует в выполнении конкретных запросов со стороны клиентов. При возникновении нештатного события в инженерной инфраструктуре, которое определяется конфигурационными параметрами, он передает информацию о событии Агенту оркестровки.

База Виртуальных Объектов содержит описания всех созданных виртуальных объектов.

База аппаратных ресурсов ЦОД содержит описание физических серверов в составе ЦОДа, на которых будут развертываться компоненты СИУ. В базу записываются: уникальный идентификатор аппаратного сервера, тип процессора, размер памяти, число и тип сетевых интерфейсов, дисковые накопители и другие параметры. Эта информация используется как при развертывании СИУ, так и при выделении ресурсов по запросам пользователей.

Репозиторий программных компонентов СИУ содержит все программные компоненты (как специально разработанные, так и заимствованные из внешних источников), которые используются в СИУ. При любых развертываниях или модернизации СИУ программные компоненты используются только из данного репозитория. За помещением всех компонентов в репозиторий отвечают на начальном этапе разработчики или в дальнейшем администраторы сопровождения СИУ. Иными словами, репозиторий должен быть единственным источником программных компонентов СИУ.

Процедура развертывания и поддержки представляет собой автоматизированный процесс развертывания и поддержки СИУ. Процесс состоит из нескольких шагов (часть ручных, часть автоматических). Первым шагом является планирование установки или модернизации СИУ. На этом шаге должны быть определены все технические параметры: доступные интервалы IP адресов, доступные интервалы MAC-адресов для виртуальных машин, распределение компонентов СИУ по имеющимся аппаратным серверам, определение сколько серверов будет выделено под виртуальные машины пользователей и сколько под системы хранения данных пользователей. Затем начинается пошаговый процесс установки компонентов СИУ с помощью разработанных скриптов установки. Результат установки очередного компонента СИУ доводится до администратора. Если очередной компонент установился успешно, то возможен старт установки следующего компонента. Если установка компоненты завершилась неуспешно, то процесс установки прерывается. Администратор должен исследовать причины, скорректировать параметры и продолжить установку. Установка системы в целом не является однократно выполняемой транзакцией.

Отметим, что передача данных между ЦОДами выполняется с использованием требований по качеству обслуживания (ТКО), которые могут включать кодирование, уплотнение, повышение устойчивости к потерям пакетов. Значительная часть функционала передачи данных реализована в виде сетевых функций.

Поскольку одним из важным компонентов СИУ являются базы данных, то для повышения надежности функционирования используется технология отказоустойчивости, основанная на конфигурировании архитектуры высокой доступности (режим мастер-мастер, где два мастера располагаются на отдельных физических серверах).

При выходе из строя отдельных аппаратных компонентов МГРЦ агентом оркестровки запускается процедура оценки ущерба, результаты которой доводятся до администратора системы, который сможет выбрать варианты действий для минимизации ущерба.

Экспериментальные исследования

Экспериментальные исследования СИУ выполнены на макете масштабируемого географически распределенного ЦОД, построенного совместно с компанией АО «СМАРТС» (г. Самара). Схема макета приведена на рис. 2.

Каждый ЦОД, представленный на рис. 2, укомплектован однотипным оборудованием, и включает:

— от 2 до 4 серверов (128GB ОП, 30 TB дисковая память, 6 сетевых интерфейсов) под управлением Naulinux.ru (гипервизор KVM), которые используются как для виртуальных машин клиентов, так и для хранения данных;

— сетевые коммутаторы, в том числе с поддержкой протокола OpenFlow;

— аппаратно-программные комплексы квантового распределения ключей.

ЦОДы объединены в единую систему волоконно-оптическим кабелем, одно из волокон которого используется для передачи квантовых ключей. Максимальное расстояние между центрами обработки и хранения данных – 100 км.

В программе исследований содержится более 40 успешно пройденных испытаний. Отметим наиболее важные из них:

— проверка возможности получения информации на экране пользователя с описанием услуг, предоставляемых пользователю МГРЦ, об отправке пользователем запросов на подключение услуг, о вводе данных для аутентификации и авторизации пользователей; проверка создания ВХД на основе подписки по запросу от Агента регистрации, авторизации и биллинга;

— проверка записи данных с VM вне МГРЦ в созданную ВХД с использованием интерфейса nextcloud. Проверка чтения данных в ВХД, записанных на VM вне МГРЦ с использованием интерфейса nextcloud;

— проверка создания VM1 и VM2 в OpenStack1(ЦОД 1) и OpenStack2 (ЦОД 2) на основе подписки по запросу от Агента регистрации, авторизации и биллинга;

- проверка входа на Аналитический портал, отображения массива информации об использовании ресурсов СИУ, логов МГРЦ, окна редактирования логических выражений шаблона;
- проверка создания правил OpenFlow виртуального канала передачи данных;
- проверка передачи данных с использованием квантового распределения ключей кодирования между парой ВМ, контроль числа переданных пакетов;
- проверка функции создания и внесения изменений в программную конфигурацию инженерных систем;
- проверка функций загрузки шаблонов запросов к СИУ в виде текстовых файлов и передачи команды на их запуск;
- проверка выполнения процедур кодирования передаваемых данных с использованием сгенерированных в квантовой системе битовых последовательностей и декодирования принимаемых данных на основе применения заимствуемых программных средств OpenSSL при отсутствии компрометации линий связи.

Указанные проверки выполнялись на основе разработанных в проекте контрольно-тестовых задач, которые были успешно завершены, что показало надежную работоспособность принятых технических решений и созданного программного обеспечения.

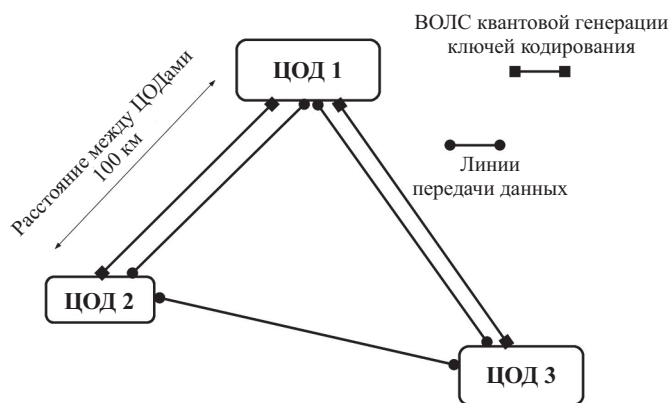


Рис. 2. Схема макета географически распределенного центра обработки и хранения данных для проведения экспериментальных исследований (ВОЛС-волоконно-оптическая линия связи)

Заключение

Представлено описание системы управления географически распределенным центром обработки и хранения данных, созданной с использованием современных архитектурных подходов и технических средств. Особое внимание уделено гибкости перестройки системы на новые задачи, эффективности использования ресурсов, надежности функционирования в условиях отказов компонентов системы и защите информации от несанкционированного доступа. Использование СИУ при проведении экспериментальных исследований на макете МГРЦ подтвердило эффективность основных принятых при разработке решений. Аппаратно-программный комплекс макета, реализованного по модели «Инфраструктура как услуга», демонстрирует отечественным операторам связи, государственным и коммерческим компаниям широкие возможности при создании ими облачных инфраструктур.

Основные преимущества созданного комплекса:

- возможности оперативного перераспределения ресурсов географически распределенного центра обработки и хранения данных как в отношении вычислительной мощности, потоков данных, так и инженерной инфраструктуры благодаря использованию концепции «инфраструктура как сервис»;
- высокая степень автономности функционирования компонентов географически распределенного центра обработки и хранения данных благодаря архитектуре на основе программных агентов, выполняющихся в операционно независимых средах;
- защищенная среда передачи данных между узлами с использованием квантовой технологии рассылки ключей кодирования в сочетании с технологией программно-конфигурируемых сетей;
- платформа для долговременного хранения и передачи больших данных, которая сформирована комбинацией используемых в системе программных компонент;
- собственный репозиторий программного обеспечения, содержащий дистрибутив Линукс и все необходимые программные пакеты (включая исходные коды), который обеспечивает автономность системы и сохранение ее работоспособности даже в случае сетевой изоляции центров обработки и хранения данных;
- автоматизированная процедура развертывания системы интегрированного управления на ресурсах центров обработки и хранения данных, не имеющая аналогов.

Литература

1. Smirnova O. Current Grid operation and future role of the Grid // *Journal of Physics: Conference Series*. V. 396. N 4. P 042055. doi:10.1088/1742-6596/396/4/042055
2. Siqi J., Baochun L. Wide area analytics for geographically distributed datacenters [Электронный ресурс]. URL: <https://ieeexplore.ieee.org/abstract/document/7442496>. Яз. англ. (дата обращения: 06.03.2019). doi: 10.1109/TST.2016.7442496
3. Bleikertz S., Kurmus A., Nagy Z.A., Schunter M. Secure Cloud Maintenance: Protecting workloads against insider attacks // *ASIACCS'12 Proc. of the 7th ACM Symposium on Information, Computer and Communications Security*. 2012. P. 83–84. doi:10.1145/2414456.2414505
4. Fedchenkov P.V., Khoruzhnikov S.E., Samokhin N.Y., Shevel A.Y. The designing of cloud infrastructure consisting of geographically distributed data centers // *Proc. of the VIII International Conference «Distributed Computing and Grid-technologies in Science and Education» (GRID 2018)*, Dubna, Moscow region, Russia, 2018. P. 32–36 [Электронный ресурс]. URL: <http://ceur-ws.org/Vol-2267/32-36-paper-5.pdf>, свободный. Яз. англ. (дата обращения: 06.03.2019).
5. Cox J.H., JR., Chung J., Donovan S., Ivey J., Clark R.J., Riley G., Owen H.L. Advancing Software-Defined Networks: A Survey // *IEEE Access*. 2017. V. 5. P. 25487–25526. doi: 10.1109/ACCESS.2017.2762291
6. Carlson M., Yoder A., Schoeb L., Deel D., Pratt C., Lionetti C., Voigt D. Software Defined Storage [Электронный ресурс]. URL: https://www.snia.org/sites/default/files/SNIA_Software_Defined_Storage_%20White_Paper_v1.pdf, свободный. Яз. англ. (дата обращения: 09.02.2018).
7. The State of Software-Defined Storage, Hyperconverged and Cloud Storage. Sixth annual market survey [Электронный ресурс]. URL: <https://www.datacore.com/document/state-of-sds-hci-cloud-storage-sixth-annual/>, свободный. Яз. англ. (дата обращения: 05.03.2019).
8. Morris K. *Infrastructure as Code: Managing Servers in the Cloud*. O'Reilly Media, 2016. 362 p.
9. Gleim A.V., Egorov V.I., Nazarov Y.V., Smirnov S.V., Chistyakov V.V., Bannik O.I., Anisimov A.A., Kynev S.M., Ivanova A.E., Collins R.J., Kozlov S.A., Buller G.S. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference // *Optics express*. 2016. V. 24. N 3. P. 2619–2633. doi: 10.1364/OE.24.002619
10. RED HAT CEPH STORAGE An open, software-defined storage platform for the cloud [Электронный ресурс]. URL: <https://www.redhat.com/cms/managed-files/st-ceph-3.2-datasheet-f15488wg-201901-en.pdf>, свободный. Яз. англ. (дата обращения: 06.03.2019).
11. Глейм А.В., Чистяков В.В., Банник О.И., Егоров В.И., Булдаков Н.В., Васильев А.Б., Гайдаш А.А., Козубов А.В., Смирнов С.В., Кынев С.М., Хоружников С.Э., Козлов С.А., Васильев В.Н. Квантовая коммуникация на боковых частотах со скоростью 1 Мбит/с в городской сети // *Оптический журнал*. 2017. Т. 84. № 6. С. 3–9.

Авторы

Хоружников Сергей Эдуардович — кандидат физико-математических наук, доцент, декан факультета, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 6508306061, ORCID ID: 0000-0003-3300-4254, xse@itmo.ru

Шевель Андрей Евгеньевич — старший преподаватель, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация; начальник отдела вычислительных систем, НИЦ «Курчатовский Институт» — ПИЯФ, Гатчина, ЛО, 188300, Российская Федерация, Scopus ID: 10045788800, ORCID ID: 0000-0002-2835-536X, Shevel.Andrey@gmail.com

References

1. Smirnova O. Current Grid operation and future role of the Grid. *Journal of Physics: Conference Series*, vol. 396, no. 4, pp. 042055. doi:10.1088/1742-6596/396/4/042055
2. Siqi J., Baochun L. *Wide area analytics for geographically distributed datacenters*. Available at: <https://ieeexplore.ieee.org/abstract/document/7442496> (accessed: 06.03.2019). doi: 10.1109/TST.2016.7442496
3. Bleikertz S., Kurmus A., Nagy Z.A., Schunter M. Secure Cloud Maintenance: Protecting workloads against insider attacks. *ASIACCS '12 Proc. of the 7th ACM Symposium on Information, Computer and Communications Security*, 2012, pp. 83–84. doi:10.1145/2414456.2414505
4. Fedchenkov P.V., Khoruzhnikov S.E., Samokhin N.Y., Shevel A.Y. The designing of cloud infrastructure consisting of geographically distributed data centers. *Proc. of the VIII International Conference «Distributed Computing and Grid-technologies in Science and Education» (GRID 2018)*, Dubna, Moscow region, Russia, 2018, pp. 32–36. Available at: <http://ceur-ws.org/Vol-2267/32-36-paper-5.pdf> (accessed: 06.03.2019).
5. Cox J.H., JR., Chung J., Donovan S., Ivey J., Clark R.J., Riley G., Owen H.L. Advancing Software-Defined Networks: A Survey. *IEEE Access*, 2017, vol. 5, pp. 25487–25526. doi: 10.1109/ACCESS.2017.2762291
6. Carlson M., Yoder A., Schoeb L., Deel D., Pratt C., Lionetti C., Voigt D. *Software Defined Storage*. Available at: https://www.snia.org/sites/default/files/SNIA_Software_Defined_Storage_%20White_Paper_v1.pdf (accessed: 09.02.2018).
7. *The State of Software-Defined Storage, Hyperconverged and Cloud Storage. Sixth annual market survey*. Available at: <https://www.datacore.com/document/state-of-sds-hci-cloud-storage-sixth-annual/> (accessed: 05.03.2019).
8. Morris K. *Infrastructure as Code: Managing Servers in the Cloud*. O'Reilly Media, 2016, 362 p.
9. Gleim A.V., Egorov V.I., Nazarov Y.V., Smirnov S.V., Chistyakov V.V., Bannik O.I., Anisimov A.A., Kynev S.M., Ivanova A.E., Collins R.J., Kozlov S.A., Buller G.S. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. *Optics express*, 2016, vol. 24, no. 3, pp. 2619–2633. doi: 10.1364/OE.24.002619
10. *RED HAT CEPH STORAGE An open, software-defined storage platform for the cloud*. Available at: <https://www.redhat.com/cms/managed-files/st-ceph-3.2-datasheet-f15488wg-201901-en.pdf> (accessed: 06.03.2019).
11. Gleim, A.V., Chistyakov V.V., Bannik O.I., Egorov V.I., Buldakov N.V., Vasilev A.B., Gaidash A.A., Kozubov A.V., Smirnov S.V., Kynev S.M., Khoruzhnikov S.E., Kozlov S.A., Vasil'ev V.N. Sideband quantum communication at 1 Mbit/s on a metropolitan area network. *Journal of Optical Technology*, 2017, vol. 84, no. 6, pp. 362–367. doi: 10.1364/JOT.84.000362

Authors

Sergey E. Khoruzhnikov — PhD, Associate Professor, Dean, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 6508306061, ORCID ID: 0000-0003-3300-4254, xse@itmo.ru

Andrey Ye. Shevel — Senior lecturer, ITMO University, Saint Petersburg, 197101, Russian Federation; Department head, Petersburg Nuclear Physics Institute named by B.P. Konstantinov of National Research Centre «Kurchatov Institute» (NRC «Kurchatov Institute» — PNPI), Gatchina, Leningrad District, 188300, Russian Federation, Scopus ID: 10045788800, ORCID ID: 0000-0002-2835-536X, Shevel.Andrey@gmail.com