Глобус

Защищённая облачная платформа

Архитектура и описание

ООО «Лаборатория 50»

e-mail: team@lab50.net

2016

Защищённая облачная платформа «Глобус»: Архитектура и описание

Настоящий документ является описанием структуры защищённой облачной платформы «Глобус». Данный документ не покрывает вопросы инсталляции. Документ сделан на основе перевода оригинала «OpenStack Cloud Administration Guide», предоставляемого организацией OpenStack Foundation.

Дата публикации: 6 апреля 2016 г.

ООО «Лаборатория 50»
198259, г. Санкт-Петербург, ул. Пограничника Гарькавого, дом 36, корп. 1, литер А, пом. 10Н

Содержание

1 Назначение

Защищённая облачная платформа «Глобус» предназначена для построения закрытых защищённых вычислительных облаков, соответствующих требованиям ФСТЭК для систем класса АС, обрабатывающих данные с грифом «секретно» и «совершенно секретно». Программное обеспечение платформы ограничивает доступ к объектам облачной инфраструктуры (виртуальные машины, образы, и т.п.) в соответствии с мандатными и ролевыми правами пользователей.

Глобус совместно с операционной системой (ОС) Astra Linux Special Edition образует систему, удовлетворяющую следующим требованиям ФСТЭК России:

1) уровень контроля отсутствия НДВ 2;
2) класс защищенности от НСД к информации 1Б.

Защищённая облачная платформа «Глобус» может быть использована для построения инфраструктуры обеспечения доступа к выделенным вычислительным ресурсам (сети, сервера, сервисы и приложения). Отличительными особенностями вычислительного облака являются скорость развёртывания, гибкость конфигурации ресурсов и обеспечения безопасности.

Облачная платформа состоит из набора компонентов со стандартизированным прикладным программным интерфейсом (API). Комбинируя состав разворачиваемой облачной инфраструктуры, возможно решать самый широкий круг задач.

Облачные системы на основе платформы Глобус могут быть эффективно использованы в следующих областях:

— виртуализация (в т.ч. замена импортного программного обеспечения);
— интеллектуальный анализ больших объёмов данных;
— потоковая передача данных;
— имитационные стенды и тренажёры;
— сервисные и справочные службы;
— отраслевые приложения;
— среды тестирования и разработки.

Решения на базе защищённой облачной платформы «Глобус» позволяют обеспечить:

— надёжность функционирования и доступность ИТ-сервисов, приложений, вычислительных мощностей;
— гибкость и оперативное масштабирование ИТ-ресурсов;
— снижение рисков при развёртывании и внедрении информационных систем;
— снижение капитальных затрат на инфраструктуру;
— упрощение и уменьшение трудоёмкости администрирования;
— ускорение разворачивания новых проектов.

В данном документе описывается архитектура облачного ПО и состав компонентов для анализа возможных вариантов решения требуемых задач.

1.1 Характеристики

Вычислительная инфраструктура, построенная на основе защищённой вычислительной платформы, обладает всеми ключевыми возможностями облаков:

— *Самообслуживание по требованию.* Потребитель самостоятельно определяет и изменяет вычислительные потребности, такие как серверное время, скорости обработки данных, объём хранимых данных без взаимодействия с представителем поставщика услуг.
— *Универсальный доступ по сети.* Услуги доступны потребителям по сети передачи данных вне зависимости от используемого терминального устройства.
— *Консолидация ресурсов.* Поставщик услуг объединяет ресурсы для обслуживания большого числа проектов (потребителей) в единый пул для динамического перераспределения мощностей между потребителями в условиях постоянного изменения спроса на мощности.
— *Эластичность.* Услуги могут быть предоставлены, расширены, сужены в любой момент времени, без дополнительных издержек на взаимодействие с поставщиком, как правило, в автоматическом режиме.
— *Учёт потребления.* Поставщик услуг автоматически исчисляет потреблённые ресурсы (объём хранимых данных, пропускная способность, количество пользователей, количество транзакций).

ПО Глобуса основано на открытой облачной платформе OpenStack. В настоящее время это одна из наиболее известных открытых облачных платформ. В разработке OpenStack участвуют более 150 компаний, среди которых Cisco, HP, Dell, AMD, Intel и NEC.

Использование платформы OpenStack обеспечивает следующие преимущества:

— Наибольшее сообщество пользователей среди открытых проектов.
— API: соответствует стандартам индустрии, доступ на основе аутентификации с ограничениями максимальной интенсивности запросов.
— Широкие возможности по конфигурации для конкретных нужд и требований.
— Поддержка Amazon EC2 и S3 API упрощает миграцию и увеличивает совместимость с другими облачными решениями.
— Распределенная и асинхронная архитектура позволяет реализовать системы с неограниченным горизонтальным масштабированием и высокой надёжностью.
— Ролевая политика избирательного управления доступом.
— Возможность изоляции проектов различных групп пользователей с квотированием ресурсов.

Глобус дополнительно предоставляет следующую функциональность:

— Единая идентификация пользователей на основе протокола Kerberos.
— Мандатное разделение доступа к виртуальным машинам, образам и томам.
— Интегрированная система аудита безопасности.
— Тесная интеграция со средствами защиты информации ОС Astra Linux Special Edition и доменом Astra Linux Directory.

1.2 Общие требования

ПО облачной платформы способно функционировать на широко распространённом оборудовании и может быть развёрнуто на основе существующей инфраструктуры. Сервера должны быть на основе процессоров с поддержкой технологии Intel VT или AMD SVM и работать под управлением ОС Astra Linux Special Edition.

Особые требования к сетевой инфраструктуре и ресурсам хранения данных не предъявляются.

Глобус предлагает различные модели организации сетевых ресурсов. Возможно использование VLAN, DHCP, IPv6 для гибкой настройки и обеспечения безопасности.

Ресурсы хранения данных могут быть как сосредоточены на выделенных системах хранения данных (СХД), так и находиться на множестве серверов в распределенной файловой системы GlusterFS.

2 Архитектура

ПО облачной платформы включает в себя ряд компонентов, предоставляющих различные функции. В основе вычислительных облаков на базе Глобуса лежит архитектура облачного стека OpenStack.

Архитектура защищённой облачной платформы предоставляет широкие возможности по конфигурации компонентов для решения различных классов задач. Для достижения этой цели каждый из составных сервисов спроектирован для предоставления «инфраструктуры как услуги» (IaaS). Интеграция достигается при помощи программных интерфейсов приложений (API), предоставляемых каждым сервисом. По большей части это тот же набор API методов, который доступен пользователям облака.

2.1 Состав облачной платформы

Защищённая облачная платформа «Глобус» включает шесть базовых сервисов: менеджер виртуальных машин, реестр образов, инструментальная панель, служба безопасности, сетевой интегратор, оператор блочных устройств. Для организации хранения данных используется сервис GlusterFS.

— *Реестр образов* предоставляет функции по созданию, управлению и контролю за образами виртуальных машин.

— *Менеджер виртуальных машин* является центральным элементом облачной инфраструктуры. Управляет виртуальными машинами.

— *Инструментальная панель* предоставляет модульный веб-интерфейс пользователя для всех сервисов облачной платформы. Панель предоставляет возможность для выполнения большинства операций в облаке.

— *Служба безопасности* выполняет функции по аутентификации и авторизации во всем облаке. Служба безопасности интегрирована с доменом Astra Linux Directory ОС Astra Linux Special Edition для обеспечения требований по НСД.

— *Сетевой интегратор* предоставляет функции по организации сети между виртуальными машинами, запущенными в облаке. С помощью сервиса пользователь может создавать сети и настраивать сетевые интерфейсы виртуальных машин.

— *Оператор блочных устройств* предоставляет доступ к блочным устройствам постоянного хранения данных гостевым ОС. Блочные устройств могут располагаться в различных физических структурах (SAN и т.\,п.).

— *Кластерная файловая система* представляет собой распределенную, параллельную, линейно масштабируемую файловую систему с возможностью защиты от сбоев. В составе защищённой облачной платформы может выполнять несколько функций: хранение образов реестра, хранение образов гостевых виртуальных машин для организации бесшовной миграции.

— *Программный коммутатор* обеспечивает маршрутизацию сетевых пакетов между виртуальными машинами. Маршруты потоков данных задаются программно и хранятся в базе данных.

Для осуществления мандатного контроля над виртуальными машинами и образами используется подсистема безопасности PARSEC операционной системы Astra Linux Special Edition.

2.2 Композитная структура

Облачная платформа «Глобус» предназначена для построения высокомасштабируемых облачных структур. Каждый компонент спроектирован таким образом, чтобы совместно с другими обеспечивать «инфраструктуру как сервис» (IaaS). Такая интеграция осуществляется посредством открытых интерфейсов прикладного программирования (API), предоставляемых каждым сервисом (и, в свою очередь, используемых другими). Несмотря на то, что компоненты тесно взаимосвязаны с другими компонентами посредством API, каждый отдельный компонент может быть заменён на другую реализацию, предоставляющую аналогичный API. По сути, API сервисов аналогичен предоставляемому пользователю.

В целом, взаимосвязь сервисов можно пояснить следующим образом (рис. 2.1):

— Инструментальная панель предоставляет интерфейс для пользователя к остальным компонентам облака.

— Менеджер виртуальных машин извлекает виртуальные диски с ассоциированными метаданными из сервиса Реестра образов.

— Сетевой интегратор предоставляет виртуальные сети для сервиса Менеджера ВМ.

— Оператор блочных устройств предоставляет доступ к блочным устройствам для сервиса Менеджера ВМ.

— Реестр образов может использовать кластерную ФС для хранения данных.

— Все сервисы используют Службу безопасности для проведения аутентификации и авторизации.

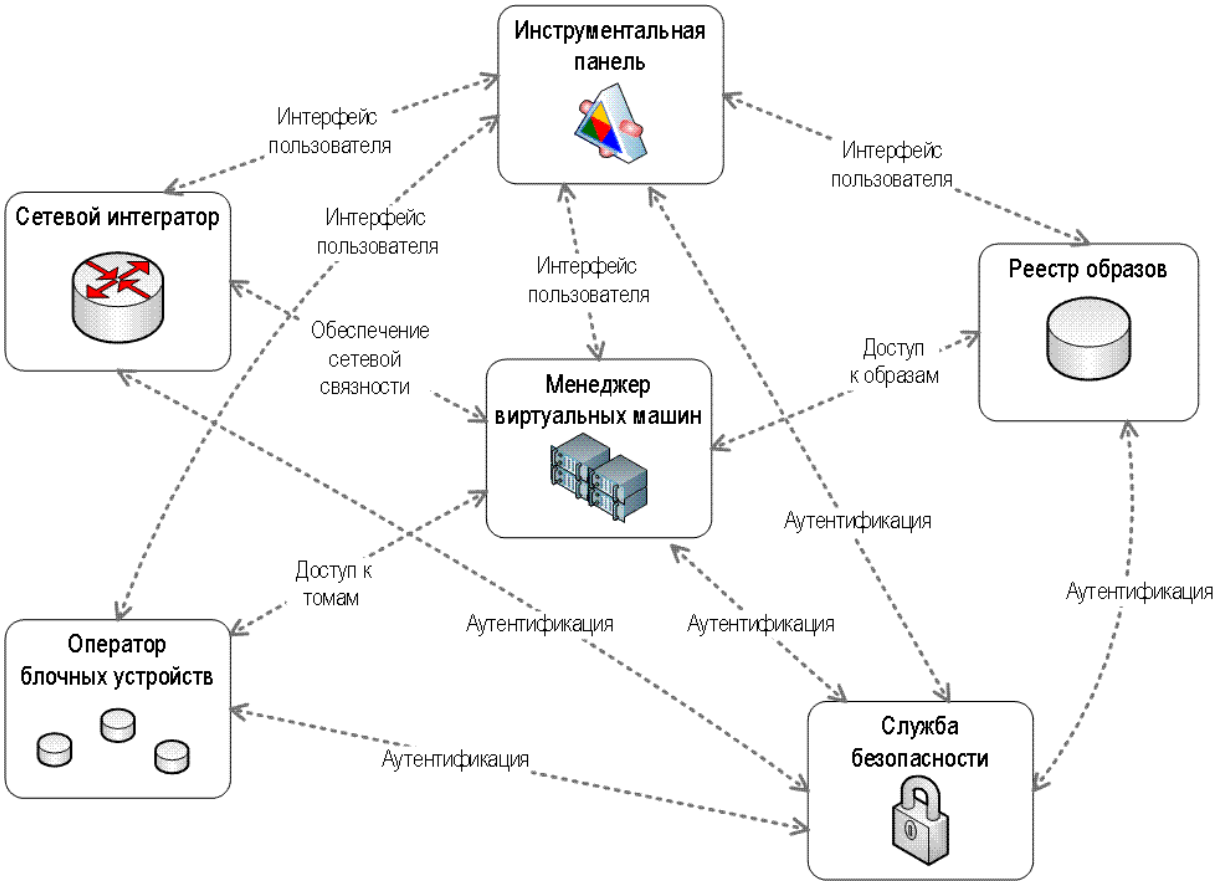

Рис. 2.1: Взаимодействие компонентов

Данное упрощённое представление предполагает, что задействованы все компоненты защищённой облачной платформы в типовых вариантах. Описанные взаимодействия между компонентами не учитывают возможного специфического использования конечными пользователями.

2.3 Совместимость с Amazon Web Services

Несмотря на то, что Глобус предназначена в первую очередь для развёртывания закрытых облаков, она включает аналоги сервисов AWS:

— Менеджер виртуальных машин концептуально выполняет функции EC2. Есть возможность использовать API совместимое с EC2.
— Кластерная файловая ФС концептуально выполняет функции S3, включает подмножество API S3.
— Реестр образов предоставляет многие функции AMI.
— Оператор блочных устройств предоставляет функции аналогичные EBS.

3 Компоненты

Детализированное представление обобщённой архитектуры показано на рис. 3.2. Данная архитектура описывает типовую конфигурацию компонентов облачной платформы. Тем не менее, Глобус обладает возможностью гибкой конфигурации для реализации требований, необходимых заказчику. На схеме не показаны вспомогательные службы и компоненты, не относящиеся непосредственно к облаку: СУБД PostgreSQL, PARSEC, Astra Linux Directory.

3.1 Инструментальная панель

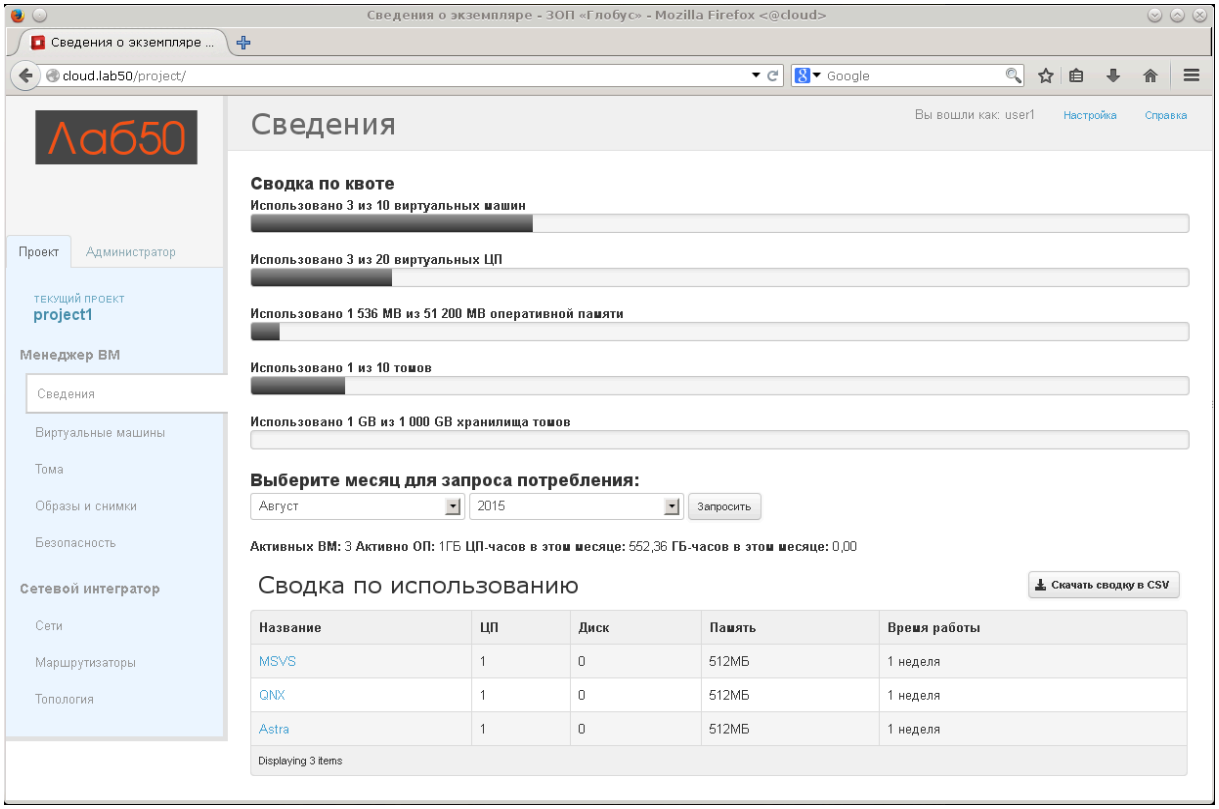

Рис. 3.1: Инструментальная панель

Инструментальная панель — это модульное веб-приложение на основе фреймворка Django. Предоставляет интерфейс пользователям и администраторам к сервисам облака.

Панель использует для функционирования mod_wsgi веб-сервера Apache. Аутентификация пользователя осуществляется веб-сервером по протоколу SPNEGO с использованием СЗИ, встроенных в Astra Linux Special Edition. Типовая конфигурация предполагает использование средств аутентификации Kerberos домена ALD. Одновременно с веб-панелью могут использоваться утилиты командной строки для взаимодействия с сервисами облака.

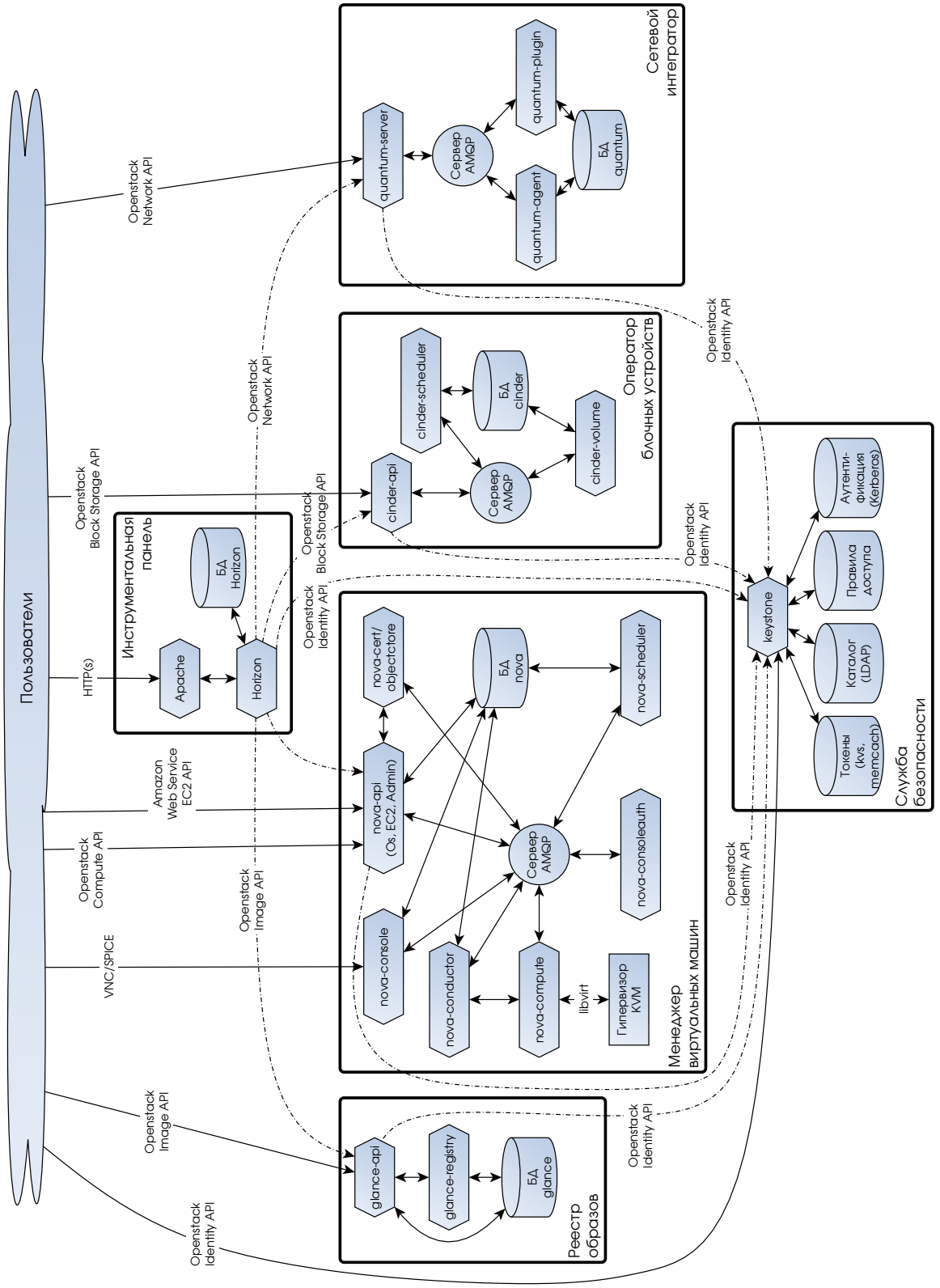

Рис. 3.2: Композитная структура

3.2 Менеджер виртуальных машин

Менеджер виртуальных машин является центральной частью облачной платформы. В свою очередь состоит из нескольких одновременно функционирующих модулей.

nova-api принимает и реагирует на запросы пользователей к сервису Nova. Поддерживает прикладные программные интерфейсы OpenStack, Amazon EC2 и специализированный API администрирования для привилегированных пользователей. Является связующим звеном облака, организует взаимодействие сервисов для выполнения многих команд пользователя. Также обеспечивает проведение некоторых проверок при проведении операций (в основном проверка квот).

nova-compute — это первичный сервис, который взаимодействует через интерфейс виртуализации libvirt с гипервизором KVM. Функциональность модуля достаточно широка, однако по сути он проводит множество манипуляций с помощью API libvirt и системных команд по входящим запросам, при этом актуализируя информацию о гостевых системах в БД.

nova-schedule выполняет функции диспетчера при создании виртуальных машин. При поступлении запроса от пользователя на создание ВМ определяет физический узел (сервер) облака, на котором она будет запущена.

nova-network является упрощённым аналогом сетевого интегратора Quantum. В простых конфигурациях может выполнять его функции.

nova-conductor организует доступ к базе данных для модулей nova-compute.

nova-console, nova-xvpvncproxy, nova-spicehtml5proxy, nova-consoleauth предоставляют доступ пользователям к их виртуальным машинам посредством создания прокси-серверов.

Взаимодействие между модулями сервиса менеджера виртуальных машин обеспечивается с помощью обмена сообщениями посредством AMQP сервера RabbitMQ (входит в состав ОС Astra Linux Special Edition).

Для хранения состояния и конфигурации облака используется СУБД PostgreSQL, входящая в состав Astra Linux Special Edition. Для повышения надёжности СУБД может быть сконфигурирована в режиме «горячего резервирования» данных на вторичном (запасном) сервере.

3.3 Реестр образов

Компонент Реестр образов предназначен для работы с образами виртуальных машин. Пользователи производят манипуляции с образами через Реестр образов, который хранит их вместе с метаданными в хранилище (как правило GlusterFS) и отвечает на запросы других компонентов облака (главным образом Nova). Авторизация пользователей осуществляется через сервис ALD ОС Astra Linux Special Edition.

Реестр образов состоит из следующих компонентов: glance-api, glance-registry и нескольких вспомогательных программ.

glance-api реализует ППИ управления образами: обзор, загрузка, выгрузка и др.

glance-registry хранит и обрабатывает образы виртуальных машин и их параметры (метаданные), сопутствующие образам.

glance-cache вспомогательные модули, следящие за доступностью, актуальностью и консистентностью кэша во всем кластере.

glance-replicator программа для переноса данных существующего реестра образа во вновь создаваемый.

glance-scrubber служит для очистки реестра от удалённых пользователями образов.

Для хранения метаданных используется СУБД PostgreSQL, входящая в состав Astra Linux Special Edition.

3.4 Служба безопасности

Служба безопасности предоставляет остальным сервисам облачной платформы информацию о проектах и правах пользователей. Авторизацию и аутентификацию сервис производит только при наличии идентификационных данных (билетов Kerberos), полученных пользователем в службе Astra Linux Directory (ЕПП).

Дополнительная информация о пользователях и группах запрашивается через службу OpenLDAP, функционирующую в составе ALD. Пользователь должен быть корректно аутентифицирован в домене ALD чтобы использовать сервисы облака.

Сервис Службы безопасности получает следующую информацию из службы ALD: пользователи, проекты, роли, роли пользователей в проектах.

Для хранения данных о развёрнутых сервисах облачной инфраструктуры используется СУБД PostgreSQL.

3.5 Сетевой интегратор

Сетевой интегратор — это самостоятельный компонент защищённой облачной платформы «Глобус». По значимости он находится в одном ряду с Менеджером виртуальных машин, Реестром образов, Службой безопасности. Аналогично другим компонентам Глобуса, развёртывание Сетевого интегратора включает размещение ряда служб на различных серверах.

Главной службой Интегратора является демон `quantum-server`, предоставляющий прикладной интерфейс и позволяющий выполнять задачи администрирования подключаемого сетевого модуля. Большинству сетевых модулей необходимо подключение к СУБД для хранения состояния.

Если конфигурация развёртывания предполагает использование выделенного централизованного узла в облаке (облачного контроллера), то он может быть использован для установки служб Сетевого интегратора. Однако Сетевой интегратор Глобуса является независимым компонентом и также может быть развернут на выделенном узле. В зависимости от желаемой конфигурации состав необходимых сетевых служб может варьироваться.

Агент сетевого модуля (`quantum-*-agent`). Необходимость в агенте определяет используемый сетевой модуль, поскольку для некоторых модуль агент не нужен. Работает на каждом узле виртуализации для предоставления услуг подключения и маршрутизации.

Агент DHCP (`quantum-dhcp-agent`). Предоставляет услугу DHCP в сетях проектов. Требуется для некоторых сетевых модулей.

Агент L3 (`quantum-l3-agent`). Обеспечивает услугу L3/NAT для выхода виртуальных машин из сетей проектов во внешнюю сеть. Требуется для некоторых сетевых модулей.

Эти агенты взаимодействуют с основным процессом (quantum-server) посредством RPC (и брокера сообщений RabbitMQ) или через стандартный ППИ. Сетевой интегратор взаимодействует через стандартный ППИ с другими компонентами Глобуса следующим образом:

— Использует Службу безопасности Глобуса для авторизации всех запросов ППИ.

— Получает запросы от Менеджера виртуальных машин для подключения виртуальных сетевых интерфейсов к определённой сети.

— В Инструментальной панели Глобуса интегрированы функции по управлению объектами Сетевого интегратора посредством веб-интерфейса.

3.6 Оператор блочных устройств

Оператор блочных устройств реализует функциональность по управлению томами и снимками томов (снапшотами). Состоит из следующих модулей: cinder-api, cinder-volume, cinder-scheduler.

cinder-api принимает запросы через API и перенаправляет в cinder-volume для выполнения.

cinder-volume взаимодействует с различными аппаратными и программными устройствами хранения данных. В настоящее время существуют драйверы для устройств IBM, SolidFire, NetApp, Nexenta, Linux iSCSI и других.

cinder-scheduler аналогично nova-scheduler выполняет функции диспетчера к устройствам-поставщикам томов.

Для хранения состояния cinder-volume используется СУБД PostgreSQL. Компоненты сервиса Оператор блочных устройств взаимодействуют посредством обмена сообщениями через AMQP сервер RabbitMQ.

3.7 Файловое хранилище

Файловое хранилище GlusterFS — это распределённая, параллельная, линейно масштабируемая файловая система с возможностью защиты от сбоев. С помощью InfiniBand RDMA или TCP/IP GlusterFS может объединить хранилища данных, находящиеся на разных серверах, в одну параллельную сетевую файловую систему. В составе облачной платформы «Глобус» файловая система адаптирована для работы с системой защиты PARSEC ОС Astra Linux Special Edition.

GlusterFS разделена на серверную и клиентскую части. На каждом сервере работает демон glusterfsd, который делает доступным для клиентов локальное хранилище в качестве тома. Клиентский процесс glusterfs соединяется с одним или несколькими серверами посредством TCP/IP или InfiniBand и объединяет все доступные серверные тома в один, используя расширяемые трансляторы (функциональные модули системы). Получившийся том монтируется на клиентском узле при помощи механизма Filesystem in Userspace.

Большая часть функциональности GlusterFS реализована в виде трансляторов (модулей). Использование необходимых трансляторов и их настройка позволяет гибко настраивать режим работы системы. Трансляторы реализуют следующую функциональность:

— синхронная репликация между серверами;

— чередование порций данных между серверами;

— распределение файлов между серверами;

— балансировка нагрузки;

— восстановление после отказа узла;

— опережающее чтение и запаздывающая запись для увеличения быстродействия;

— дисковые квоты.

Помимо файлового интерфейса, GlusterFS предоставляет интерфейс для объектного доступа (API OpenStack) аналогичный Amazon S3.

3.8 Библиотека управления виртуализацией

Библиотека управления виртуализацией предоставляет единый интерфейс управления над широкой номенклатурой гипервизоров. Версия, включённая в ЗОП «Глобус», предназначена для работы с гипервизором KVM и доработана для обеспечения мандатного разграничения доступа к контролируемым виртуальным машинам.

libvirt предоставляет интерфейс двух видов:

— интерфейс командной строки посредством командной оболочки virsh;

— прикладной программный интерфейс на языках Питон и Си.

Посредством данного интерфейса можно создавать и управлять виртуальными машинами, настраивать состав виртуальных аппаратных средств, управлять подключаемыми томами.

Возможности ППИ libvirt охватывают все функции, необходимые для развёртывания и управления виртуальными машинами. Это влечёт за собой требования по управлению гипервизором и ресурсами, необходимыми для виртуальных машин, такими как сети, устройства хранения данных и физическими PCI/USB-устройствами. Большинство функций ППИ, предоставляемых libvirt, имеют подключаемые внутренние драйверы, позволяя поддерживать различные базовые технологии виртуализации и операционные системы. Таким образом, номенклатура функций, доступных через ППИ определяется конкретным драйвером гипервизора и возможностями используемой базовой технологии виртуализации.

Поскольку виртуальная машина является обычным процессом операционной системы, то встроенные средства защиты ОС Astra Linux Special Edition применяются в полной мере. Запускаемый привилегированным пользователем процесс QEMU, согласно политики КСЗ, получает соответствующую мандатную метку.

3.9 Программный коммутатор

Программный коммутатор обеспечивает маршрутизацию сетевых пакетов между виртуальными машинами. Маршруты потоков данных задаются программно и хранятся в базе данных.

Программный коммутатор построен по модульному принципу и состоит из нескольких компонентов.

ovs-vswitchd совместно с модулем ядра openvswitsh осуществляет маршрутизацию сетевых потоков. Реализован как демон, функционирующий на всех узлах облачной инфраструктуры.

ovsdb-server является простой СУБД, хранящей параметры, запрашиваемые ovs-vswitchd.

3.10 Гипервизор KVM

Гипервизор KVM обеспечивает виртуализацию в среде Astra Linux Special Edition на платформе x86 на основе аппаратной виртуализации Intel VT или AMD SVM. KVM обеспечивает аппаратную виртуализацию для гостевых систем.

Каждая гостевая операционная система представляет собой отдельный процесс базовой операционной системы. Процесс KVM имеет изолированное от других гостевых процессов адресное пространство. Гипервизор использует аппаратные возможности для виртуализации процессора и программные — для виртуализации памяти. При наличии процессора с поддержкой виртуализации памяти (AMD NPT или Intel EPT) KVM может использовать аппаратные средства.

Выполнение операции ввода/вывода с гостевой операционной системы обеспечивается QEMU. QEMU — платформа виртуализации, которая позволяет эмулировать широкий спектр оборудования (включая диски, графические адаптеры, сетевые устройства). Любые запросы ввода/вывода, которые делает гостевая операционная система, перехватываются и направляются в пользовательский режим для эмулирования с помощью процесса QEMU.

Гипервизор KVM предоставляет возможность работы гостевой операционной системы с паравиртуальными устройствами. В этом случае гостевые операционный системы должны использовать паравиртуальные драйвера, обеспечивающие повышенную пропускную способность и уменьшающие задержки дискового и сетевого ввода-вывода.

В настоящее время доступны паравиртуальные драйвера для следующих гостевых ОС:

— «Astra Linux» (Common Edition и Special Edition);
— Red Hat Enterprise Linux версии 4.8 и выше;
— Linux с версиями ядра более 2.6.27;
— Windows XP (x86);
— Windows Server 2003 (x86, x86 64);
— Windows Server 2008 (x86, x86 64);
— Windows 7 (x86, x86 64).

Для повышения изоляции процессов гостевых ОС и разграничения доступа пользователям может быть использовано мандатное разграничения доступа к процессам гипервизора. В этом режиме на процесс гипервизора и образ ВМ устанавливаются дополнительные мандатные атрибуты. Управление ВМ и удалённое подключение по протоколам VNC и SPICE в этом случае возможно только для пользователей с идентичными мандатными атрибутами.

Основные характеристики гипервизора:

— Поддержка аппаратной виртуализации и паравиртуальных устройств для гостевых систем.
— Поддержка технологий виртуализации MMU (AMD NPT и Intel EPT).
— Возможность работы с оборудованием из гостевой ОС (AMD IOMMU, Intel VT-D, SR-IOV).
— Мандатный доступ к процессам гостевых ОС.
— Поддержка устройств USB 2.0.
— Защищённый доступ к гостевым ОС по протоколам VNC и SPICE.
— Поддержка технологий повышенной аппаратной защиты NX и SMEP.

Ограничения гипервизора KVM для гостевых ОС:

— до 64 виртуальных процессоров;

— в режиме полной виртуализации до 4 IDE устройств;
— эмуляция до 28 паравиртуальных устройств.