

Облачная среда «Асперитас»
Краткое руководство пользователя

Данный документ или его копии не может распространяться (полностью или частично) в любом формате без письменного разрешения ИСП РАН.

1. Описание основных функциональных возможностей облачной среды «Асперитас»

«Асперитас» предназначен для организации управления ресурсами серверов виртуализации, сетевой инфраструктурой и программно-определяемой системой хранения данных. «Асперитас» является многокомпонентной распределённой облачной средой с единой политикой безопасности.

Серверы виртуализации, с которыми работают пользователи (операторы), объединены в единую группу. Администрирование выполняют администраторы, используя специализированный сервер, предназначенный для управления и сопровождения.

На каждом сервере виртуализации работает программное обеспечение, предназначенное для создания и исполнения виртуальных машин (ВМ), внутри которых могут размещаться программные системы.

«Асперитас» предоставляет возможность разделения операторов по различным зонам видимости и с различными возможностями в рамках зон видимости. Права, выданные в рамках одной зоны видимости («проект») действуют только в рамках данной зоны видимости. Также существует возможность разделения на независимые пространства пользователей («домены») в рамках которых операторы никак не связаны между собой (то есть могут существовать пользователи с одинаковыми именами, но не связанные между собой).

Основные функциональные возможности облачной среды «Асперитас».

1. Отчуждаемость решений (возможность воссоздания инфраструктуры в изолированной среде с полным контролем над ней за счёт использования открытых стандартов, свободного ПО и научных разработок ИСП РАН).
2. Высокий уровень безопасности (среда построена на уменьшенной кодовой базе и использует собственные решения по усилению безопасности, включая UEFI-прошивку с защищённой средой выполнения и настраиваемой поддержкой проверки целостности Windows и Linux виртуальных машин).
3. Управление виртуальными сетями и вычислительными кластерами с использованием систем Keystone, Neutron, Nova (аналог Amazon EC2).

4. Блочное хранение данных, а также расширяемое объектное хранилище на основе распределённой файловой системы Ceph.
5. Возможность адаптации под решение конкретных классов задач (решение задач механики сплошных сред, анализ больших данных, анализ программ на уязвимости и др.).

Минимальные системные требования:

а) 1 сервер или рабочая станция - узел развертывания:

1. Сетевая карта с 2 портами пропускной способностью 10 Гбит/с.
2. 150 ГБ дискового пространства.
3. 8 процессорных ядер архитектуры x86_64.
4. 64 ГБ ОЗУ.

б) Контроллеры. 3 сервера для масштабов 1-20 узлов виртуализации.

1. 32 процессорных ядра архитектуры x86_64.
2. 192 ГБ ОЗУ.
3. 512 ГБ дискового пространства, SSD.
4. Сетевая карта с 2 портами пропускной способностью 10 Гбит/с на каждом узле.
5. Выделенный интерфейс IPMI, iDRAC или iLO (версии не ниже 5).

в) Узлы виртуализации:

1. Возможность аппаратной виртуализации.
2. 16 процессорных ядер архитектуры x86_64.
3. 96 ГБ ОЗУ.
4. 1ТБ дискового пространства.
5. Сетевая карта с 2 портами пропускной способностью 10 Гбит/с на каждом узле.
6. Выделенный интерфейс IPMI, iDRAC или iLO (версии не ниже 5).

Для организации блочного хранения данных и развертывания объектного хранилища дополнительно требуется:

г) 4 сервера с максимально идентичными характеристиками, а также одинаковыми по объему дисками:

1. 24 процессорных ядра архитектуры x86_64.
2. Память: 128ГБ ОЗУ.
3. Диски: 12 дисков SATA HDD, 8Тб каждый.
4. Диски: 250 ГБ дискового пространства для операционной системы.
5. Диски: 2 NVMe/M.2/SATA SSD 256 Гбайт для журналов.
6. Сеть: два порта пропускной способностью не менее 10Гбит/с.

Коммутатор 1:

1. Не менее 24 портов с пропускной способностью 10Гбит/с (или выше)
2. Поддержка 802.1q

Коммутатор 2 (управления):

1. Портов по числу серверов + 1, пропускной способностью 1Гбит/с
2. Поддержка 802.1q

Облачная среда «Асперитас» разрабатывается на языках программирования: Python, ansible, golang, C/C++. Облачная среда Asperitas разработана на базе программного обеспечения с открытым исходным кодом Openstack (лицензия Apache версии 2.0) и использует в своей работе программное обеспечение с открытым исходным кодом Serp (лицензия LGPL версия 3.0).

2. Лицензирование и установка

По вопросам определения стоимости, приобретения и использования, обращайтесь по адресу asperitas@ispras.ru.

2.1. Системные требования

Минимальные системные требования описаны в разделе 1 данного руководства.

2.2. Установка облачной среды

Область применения

К основным задачам, которые способен решать облачный дистрибутив

«Асперитас», относятся:

- развертывание частных облачных сред на физических серверах в условиях отсутствия подключения к интернету;
- развертывание надежной системы хранения;
- развертывание и предоставление сервиса оркестрации Michman.

Схема развертывания облачной среды «Асперитас»

Развертывание состоит из следующих шагов (более подробно пункты будут описаны в «Инструкция по развертыванию облачной среды»):

- подготовка аппаратного оборудования, настройка сетевого взаимодействия для корректного развертывания облачной среды «Асперитас»;
- определение ролей узлов, выделение узла развертывания;
- установка системы с диска облачного дистрибутива «Асперитас»;
- запуск сценария установки сервисов, необходимых для узла развертывания;
- если о какой-либо из машин неизвестны параметры количества ЦПУ, размера памяти дисковой и оперативной, то необходимо провести предварительный сбор данных об узлах с узла развертывания;
- конфигурация развертывания системы хранения данных. На данном этапе необходимо настроить параметры настройки сетей и работы с блочными устройствами;
- запуск процесса развертывания надежной файловой системы (ФС);
- запуск процесса развертывания облачной среды;
- запуск процесса развертывания инструмента оркестрации Michman, а также системы мониторинга.

Для полного функционирования облачной среды «Асперитас» необходим следующий набор физических узлов:

- узел развертывания. Представляет собой узел, необходимый на этапах развертывания остальных частей облачной среды «Асперитас», а также при обновлении и изменении остальных функциональных частей;
- узлы хранения. Содержат множество дисков и большое количество дискового пространства, а также представляют собой систему надежного хранения пользовательских данных в облачной среде «Асперитас». Количество должно составлять не менее 4-х;
- узлы вычислительные. Содержат все запущенные ВМ. Количество их оперативной памяти (ОП), дискового пространства и ЦПУ является вычислительной мощ-

ностью облачной среды «Асперитас»;

– узлы управления. Являются центром управления вычислительными узлами и центром общения с узлами хранения. При полной выводе из строя узлов управления запущенные ВМ продолжают свое функционирование.

Узлы управления предоставляют пользователю-оператору контроль над облачными ресурсами: их созданием, изменением и удалением. Узлы хранения позволяют надежно хранить информацию на дисках, созданных пользователем. Вычислительные узлы являются основным нагрузочным элементом, так как содержат динамически распределенные виртуальные машины пользователей.

Основные возможности инструментов развертывания Асперитас

Функциональными элементами облачной среды «Асперитас» являются:

- распределенная сеть хранения данных;
- системы хранения облачных образов, настройки виртуальных сетей, запуска ВМ и др. на базе OpenStack;
- инструмент оркестрации Michman;
- инструмент мониторинга.

Облачный дистрибутив «Асперитас» позволяет автоматизированно развертывать указанные выше функциональные элементы, а также централизованно с узла развертывания проводить обновление элементов и изменение элементов при необходимости.

Инструмент мониторинга предоставляет централизованное отслеживание сбоев и ошибок на узлах, а также централизованное отслеживание статуса ВМ, запущенных в облачной среде «Асперитас».

Примеры разработанных модулей

Разрабатываются модули, отвечающие за:

- запуск ВМ в ОС;
- развертывание надежной распределенной ФС;
- развертывание облака ВМ;

Тестовый сценарий работы с средой развертывания

Проверка работоспособности частично проводится во время развертывания облачной среды «Асперитас» при инициализации сервисов и некоторых облачных ресурсов. Во время развертывания проходят инициализация баз данных (БД) облачных сервисов, что не позволяет завершить процесс развертывания при возможных ошибках БД.

Проверяется доступность узлов другими узлами в каждой сети, настроенной на физических узлах. А затем настраивается сервис для высокой доступности сервисов, который гарантирует корректное функционирование сервисов балансировки, БД Galera, БД OVN, сервиса обмена сообщениями между системами облачной среды RabbitMQ и доступность виртуальных IP адресов.

Создаются проекты, домены, пользователи сервисов и их роли, что невозможно без корректного функционирования сервиса аутентификации.

По завершении развертывания выполнить с узла развертывания скрипты проверки облачной платформы. Выполнить команды из консоли:

```
$ source overcloudrc
$ cd cloud-prepare-scripts/playbooks
```

Файл `roles/check-nova-network/vars/main.yaml` содержит настраиваемые параметры. Обратите внимание на переменную `network_1` и ее настройки. Для функционирования этой виртуальной сети в облаке необходимо, чтобы на коммутаторах, к которым присоединяются узлы управления и вычислительные узлы, был заведен VLAN 450 в режиме `tagged` для портов узлов управления и вычислительных узлов. А также в сети `10.100.148.0/22` должен был поднят DHCP-сервер с адресом `10.100.151.254`, маршрутизирующий пакеты тегированные числом 450 и маршрутизирующий пакеты в сеть Интернет.

Запустить скрипт создания тестовых ресурсов:

```
$ ansible-playbook check-nova-network.yaml
```

При успешном выполнении данного скрипта на экране отобразится сообщение «Execute: ping <test ip>» и IP-адрес тестовой машины вида `10.100.150.*`. Чтобы протестировать доступность тестовой машины, добавить маршрутизацию из сети доступа к узлу развертывания в сеть `10.100.148.0/22`. Затем выполнить с узла развертывания:

```
$ ping <test ip>
$ ssh cirros@<test ip>
```

Последняя команда подключит к консоли тестовой машины, с которой можно выполнить некоторые действия. Например, проверить доступность сети или любого другого адреса:

```
$ ping 8.8.8.8
```

В случае если недоступен IP адрес тестовой машины, то убедиться, что адрес `10.100.151.254`. Так как самая частая причина – это неправильная настройка маршрутизации.

Если проблема не в этом, то зайти в графический интерфейс облака по адресу 10.100.144.100. Логин/пароль – admin/пароль, указанный при развертывании системы. Зайти во вкладку «Project – Compute – Instances». Нажать на VM testing_config и затем выбрать вкладку VNC. Так как это тестовая машина, то она запущена из системы Cirros с заранее заданными пользователем/паролем, указанными на экране.

Проверить, что VM получила имя хоста, равное testing_config. Получила внутренний адрес из сети 192.168.33.0/24 и маршрут по умолчанию через 192.168.33.1. При отсутствии любого из пунктов необходимо посмотреть логи neutron на узлах управления и вычислительных и устранить указанные там ошибки. А также проверить, что все завершенные контейнеры завершены со статусом 0.

В случае, если выше указанное, работает, то ошибку искать в связности и настройках сети, соответствующей VLAN 450.

Если ошибка произошла при создании образа Cirros, то посмотреть логи Glance на узлах управления и исправить указанные ошибки.

Если ошибка произошла при создании VM, то посмотреть логи Nova на узлах управления и вычислительных узлах и исправить указанные ошибки.

В предыдущих двух случаях также возможны ошибки со стороны системы хранения. Если в логах указаны ошибки обращения к узлам хранения, то посмотреть логи на узлах хранения и исправить указанные ошибки.

2.3. Инструкция по развертыванию облачной среды

Ниже описаны требования к физическим устройствам и настройкам сети, необходимым для развертывания облачной сред, а также содержится инструкция по развертыванию облака контейнеров и облака VM с использованием распределенной ФС.

2.3.1. Требования к настройке сетей на физических машинах

На всех узлах необходимо наличие сетей, указанных на рис. 1. Наличие каждой из сетей имеет свои свойства и требования. На рис. 1 не указаны сети IPMI/iDRAC. Управление через IPMI и iDRAC требуется от узлов хранения, управления и вычислительных узлов. От узла развертывания требуется доступ к этой сети для управления указанными узлами.

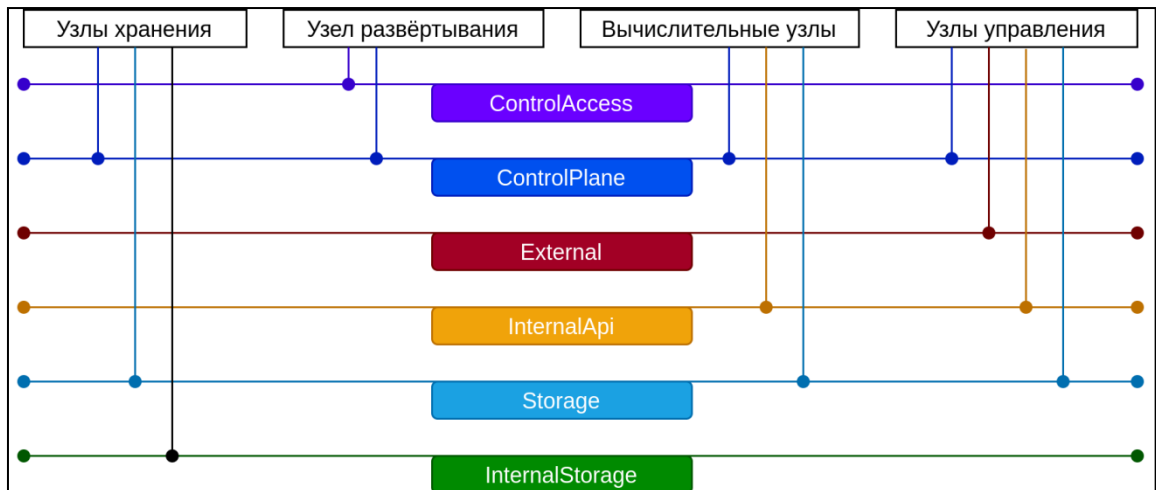


Рис. 1. Схема используемых сетей

Узел развертывания должен иметь два интерфейса, один интерфейс настраивается для доступа к узлу из сети предприятия. Ограничений для этой сети нет. И второй интерфейс должен быть без каких-либо настроек сети. Порт соответствующего интерфейса на коммутаторе должен находиться в режиме untagged для некоторого ControlPlaneVLAN, например, 10.

Узлы управления и вычислительные узлы должны иметь по два интерфейса, каждый из которых также имеет соответствующий порт на коммутаторе в режиме hybrid с ControlPlaneVLAN в качестве access. То есть весь нетегированный трафик, проходящий через эти интерфейсы на коммутаторе должен помечаться ControlPlaneVLAN.

Узел хранения должен иметь один интерфейс в режиме hybrid с ControlPlaneVLAN в качестве access и еще три интерфейса в режиме untagged для некоторого InternalStorageVLAN.

На коммутаторах, связывающих узлы управления, хранения и вычислительные узлы завести ExternalVLAN, InternalAPIVLAN, StorageVLAN и добавить их соответствующим портам.

Сеть сопровождения облака (ControlPlane). Эта сеть настраивается на узле развертывания на этапе настройки и поднятия сервисов, необходимых для развертывания остальной части облачной среды «Асперитас». После этого на узле развертывания поднимается DHCP-сервер для раздачи адресов остальным узлам облачной среды из сети 192.168.24.0/24.

IP-адрес узла развертывания в этой сети – 192.168.24.1, 192.168.24.2, 192.168.24.3.

Сеть используется для общения между узлом развертывания и облачной

средой в процессе развертывания. В дальнейшем используется как служебная сеть облачной среды «Асперитас».

Внешняя сеть доступа к облачной среде «Асперитас» (External). В сети должен существовать маршрутизатор с адресом 10.100.147.254. По этой сети пользователи облачной среды получают публичный доступ к облачным сервисам. Используемый для доступа основной адрес – 10.100.144.100

Сеть с зоной видимости внутри облачной среды для внутренних коммуникаций (InternalAPI) 172.16.2.0/24.

Сеть для доступа облачных сервисов к системе хранения (Storage) 172.16.1.0/23, адреса из этой сети – точки входа в распределенной системе хранения для клиентов.

Сеть настройки системы хранения и синхронизации – (InternalStorage)172.16.3.0/24.

Для функционирования надежной ФС необходимо наличие двух сетей – внутренней и публичной. Рекомендуемая пропускная способность для обеих сетей 10 Гбит/с или выше. Также рекомендуется поддержка больших размеров кадра (jumboframes) на коммутационном оборудовании.

2.3.2. Подготовка узла развертывания

Узел развертывания обязан иметь два интерфейса. Интерфейс для доступа к узлу настраивается исходя из требований секретности компании.

2.3.3. Развертывание облачной среды

Выполнение установки облачной среды при помощи инсталлера:

– скачать на рабочую станцию образа undercloud.iso:
http://windtrap:82/image/images/iso/undercloud.x86_64.iso;

– подключить Virtual Media – Virtual Storage (выбрать образ и нажать [Plug in])

(рис. 2):

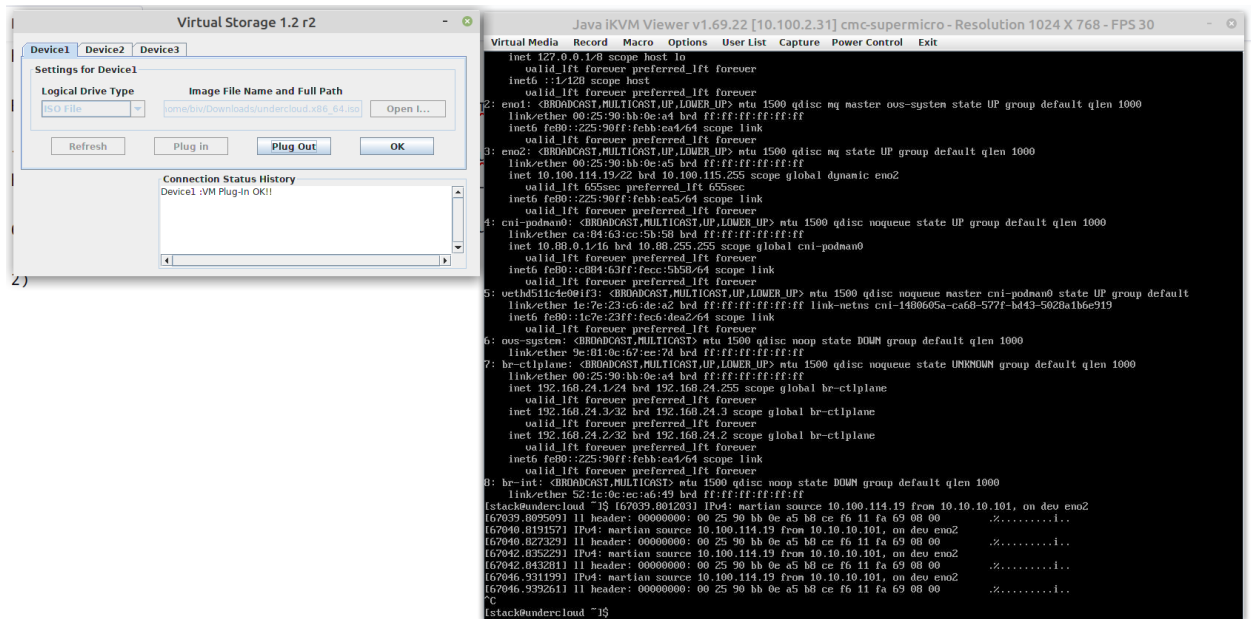


Рис. 2

– <F2> при перезагрузке узла, в BIOS меняем boot order так, чтобы загрузка шла с виртуального устройства;

– Install Aspertas, загрузка идет очень долго, один процент в ~10 мин, скорее всего из-за способа подключения через Virtual storage, при деплое с qemu или с флешки с iso деплой быстрее;

– на все вопросы нажать [ok], выбирая параметры по умолчанию. Задать только Dns сервер ИСП (10.10.12.7), поле ntp server оставить пустым;

– после установки undercloud, зайти в систему (логин stack, пароль);

– (optional) Если ввести команду ip a: на 2 интерфейсе выполнилось автоматическое назначение IP адреса в 112 влане, получив его с DHCP сервера можно поменять его вручную на другой:

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-eno2
```

здать статически адрес, sudo ifdown eno2; sudo ifup eno2, добавить необходимые маршруты, например:

```
sudo ip ro add default via 10.100.115.254 dev eno2
```

тогда на узел можно зайти по ssh по указанному IP (рис. 3).

```

[stack@undercloud ~]# I67545.6552931 IN=en02 OUT= MAC=00:25:90:bb:0e:a5:b8:ce:f6:11:fa:69:08:00 SRC=10.100.115.254 DST=10.100.11
4.19 LEN=336 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=67 DPT=68 LEN=316
I67545.6731881 IN=en02 OUT= MAC=00:25:90:bb:0e:a5:b8:ce:f6:11:fa:69:08:00 SRC=10.100.115.254 DST=10.100.114.19 LEN=336 TOS=0x10
PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=67 DPT=68 LEN=316
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master ous-system state UP group default qlen 1000
    link/ether 00:25:90:bb:0e:a4 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::225:90ff:febb:ea4/64 scope link
        valid_lft forever preferred_lft forever
3: eno2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:25:90:bb:0e:a5 brd ff:ff:ff:ff:ff:ff
    inet 10.100.114.19/22 brd 10.100.115.255 scope global dynamic eno2
        valid_lft 306sec preferred_lft 306sec
    inet6 fe80::225:90ff:febb:ea5/64 scope link
        valid_lft forever preferred_lft forever
4: cni-podman0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether ca:84:63:cc:5b:58 brd ff:ff:ff:ff:ff:ff
    inet 10.88.0.1/16 brd 10.88.255.255 scope global cni-podman0
        valid_lft forever preferred_lft forever
    inet6 fe80::c884:63ff:fecc:5b58/64 scope link
        valid_lft forever preferred_lft forever
5: vethd51c4e0eif3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master cni-podman0 state UP group default
    link/ether 1e:7e:23:c6:de:a2 brd ff:ff:ff:ff:ff:ff link-netns cni-1480605a-ca68-577f-bd43-5028a1b6e919
    inet6 fe80::1c7e:23ff:fec6:dea2/64 scope link
        valid_lft forever preferred_lft forever
6: ous-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 9e:81:0c:67:ee:7d brd ff:ff:ff:ff:ff:ff
7: br-ctlplane: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 00:25:90:bb:0e:a4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.24.1/24 brd 192.168.24.255 scope global br-ctlplane
        valid_lft forever preferred_lft forever
    inet 192.168.24.3/32 brd 192.168.24.3 scope global br-ctlplane
        valid_lft forever preferred_lft forever
    inet 192.168.24.2/32 brd 192.168.24.2 scope global br-ctlplane
        valid_lft forever preferred_lft forever
    inet6 fe80::225:90ff:febb:ea4/64 scope link
        valid_lft forever preferred_lft forever
8: br-int: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 52:1c:0c:ec:a6:49 brd ff:ff:ff:ff:ff:ff
[stack@undercloud ~]#

```

Рис. 3

– ssh к узлу, выполнить команду (рис. 4):

```
asperitas
```

```

[stack@undercloud ~]# asperitas
{'debug': False, 'log_path': '/home/stack', 'rc_path': '/home/stack/stackrc', 'images_path': '/home/stack/images-asperitas'}
Wait uploading images from path: /home/stack/images-asperitas

```

Рис. 4

– в появившемся меню выбрать Installation (рис. 5);

```

[ISP RAS] Asperitas
Menu
Installation
Configuration
Description
Manage Asperitas installation

```

Рис. 5

– заполнить параметры (рис. 6);

```

Baremetal node Details
Name: a3contr1
BMC type: [IPMI]
BMC address: 10.100.2.14
BMC login: ADMIN
BMC password: *****
Profile: [Controller]
UEFI boot mode: [ ] set if UEFI boot mode is used
PXE port mac_address: ac:1f:6b:1a:6b:7c
Disk capacity (Gb):
Cpu number:
Architecture: x86_64
Memory capacity (Mb):
Order NICs: nic1: ac:1f:6b:1a:6b:7c (Example)
             nic2: ac:1f:6b:1a:6b:7d nic1: 00:00:00:00:00:00
             nic2: 11:11:11:11:11:11
Root disk: "" (Example)
              {"serial": "123456789"}

```

Рис. 6

– старт интроспекции (рис. 7);

```

Introspection
Choose nodes to be introspected
 a3contr1 ✓ Introspection result < Refresh >
Ordered NICs:
  nic1: ac:1f:6b:1a:6b:7c
  nic2: ac:1f:6b:1a:6b:7d
Root Device: ''
error: null
finished_at: null
id: 6acc17f4-4163-4d9b-bfb2-7968b403f48d
started_at: '2022-06-08T19:01:46'
state: starting

```

Рис. 7

– по окончании первого этапа интроспекции (по окончании интроспекции выполняются поля с cpu и появится статус finished), в статусе один флаг. Выбрать root disk во вкладке introspection (второй флаг), и порядок интерфейсов. Например, eno1, eno2 (третий флаг). После получения 3 флагов, узел готов к деплою (статус Available) (рис. 8);

Baremetal nodes List					
Name	Available	Role	Cpus	Ram(Mb)	Disk(Gb)
a3contr1	No	control	32	131072	118

Introspection	
Choose nodes to be introspected	Introspection result
<input type="checkbox"/> a3contr1	✓ ✓ ✓ < Refresh >
	Ordered NICs:
	nic1: ac:1f:6b:1a:6b:7c
	nic2: ac:1f:6b:1a:6b:7d
	Root Device:
	serial: B0032004020030002
	error: null
	finished_at: '2022-06-08T19:35:47'
	id: 6acc17f4-4163-4d9b-bfb2-7968b403f48d
	started_at: '2022-06-08T19:30:38'
	state: finished

Рис. 8

– настроить сеть (рис. 9);

Name	VLAN	CIDR	MTU	Roles
Ctlplane		192.168.24.0/24	1500	["Controller", "Compute", "CephStorage"]
External	112	10.100.112.0/22	1500	["Controller", "Compute"]
InternalApi	22	172.16.3.0/24	1500	["Controller", "Compute", "CephStorage"]
Storage	30	172.16.9.0/24	1500	["Controller", "Compute", "CephStorage"]
InternalCeph	31	172.16.2.0/24	1500	["CephStorage"]
IroniProvisi...	21	192.16.7.0/24	1500	["Controller", "Compute"]

Network plan for Compute	[single-nic-vlans
Network plan for Controller	[single-nic-vlans
Network plan for CephStorage	[single-nic-linux-bridge-vlans

Рис. 9

– нажать [Deploy Openstack] в корне меню, проверить параметры и нажать [deployment] (рис. 10);

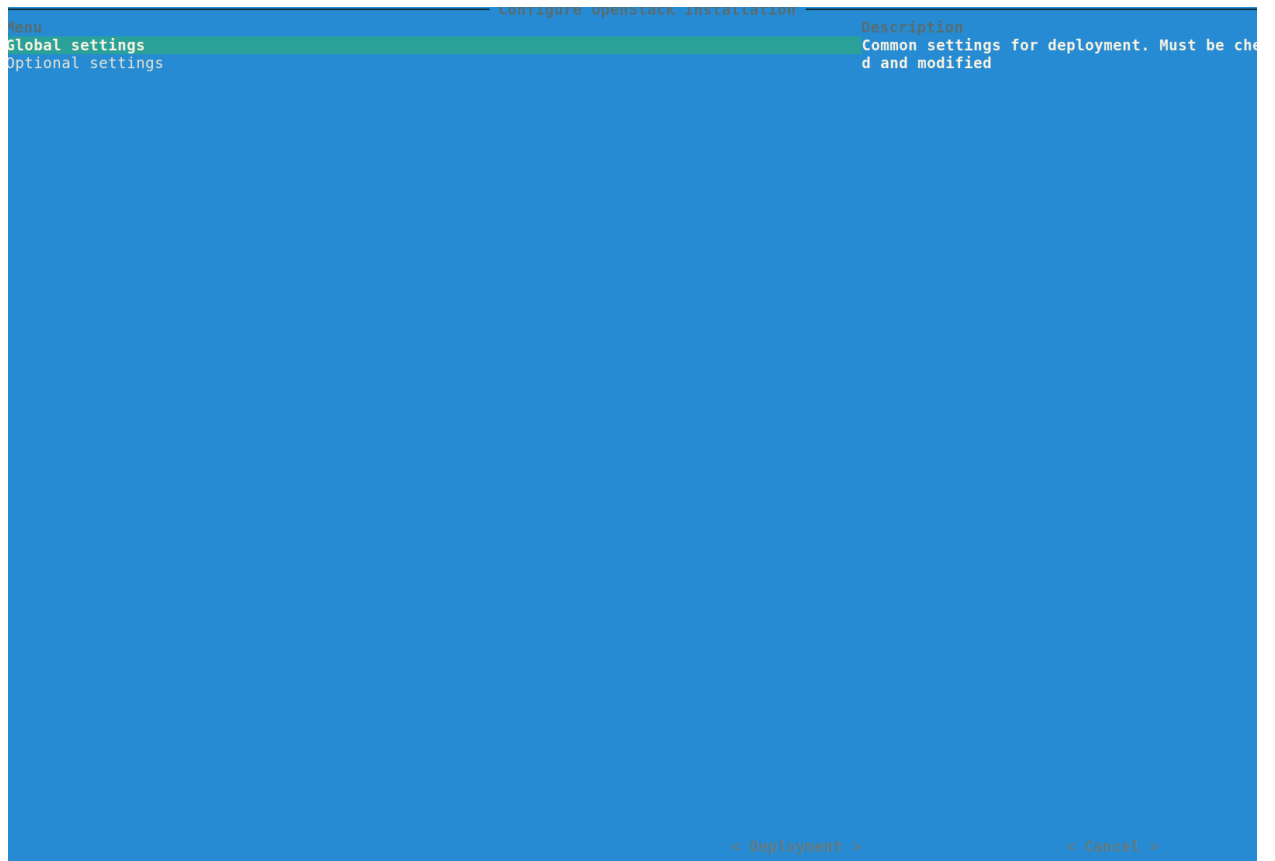


Рис. 10

– нажать [start], следить за процессом развертывания (рис. 11);

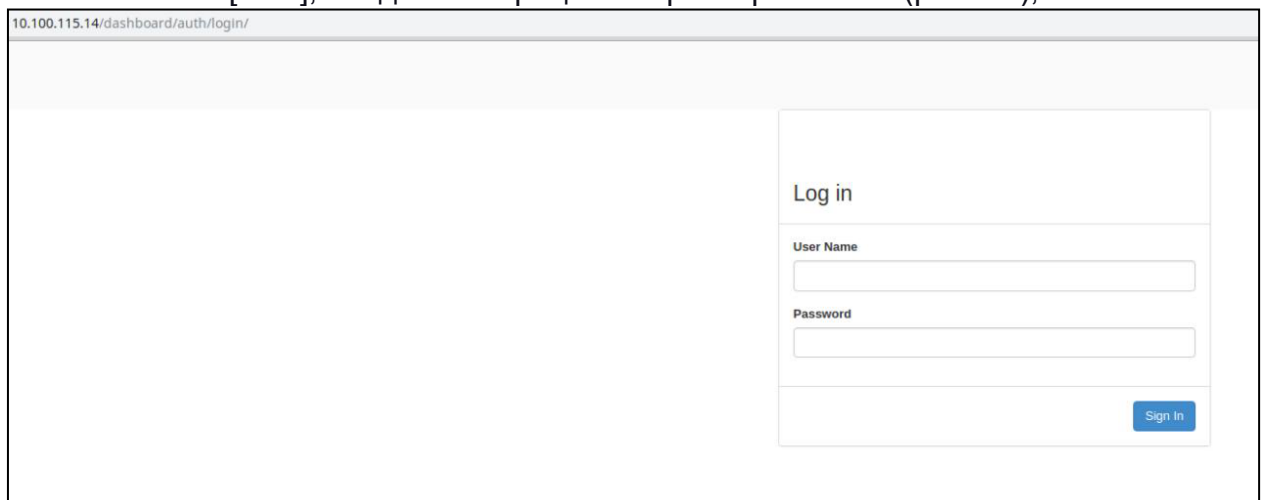


Рис. 11

2.2.4. Первичная настройка облачной среды

Используя клиент командной строки – создание типа инстанса:

```
openstack flavor create --ram 1024 --disk 10 --ephemeral 0 --
swap 0 --vcpus 1 t2.micro
```

Загрузка образа VM:

```
openstack image create --disk-format qcow2 --file cirros-
```

```
0.4.0-x86_64-disk.img cirros-0.4.0-x86_64
```

Создание ключевой пары:

```
openstack keypair create --public-key .ssh/id_rsa.pub
undercloud_key
```

Создание внутренней сети:

```
openstack network create --external --provider-network-type
geneve --provider-segment 5555 internal
```

Создание внутренней подсети:

```
openstack subnet create --dhcp --network internal --
allocation-pool start=192.168.33.5,end=192.168.33.250 --gateway
auto --subnet-range 192.168.33.0/24 internal_subnet
```

Создание роутера для внешней сети:

```
openstack router create --external-gateway external router_1
openstack router add subnet router_1 internal_subnet
```

Создание правила группы безопасности для доступа к VM по ssh:

```
openstack security group create ssh_access
openstack security group rule create --ingress --dst-port 22 -
-protocol tcp --remote-ip 0.0.0.0/0 ssh_access
openstack security group rule create --ingress --protocol icmp
--remote-ip 0.0.0.0/0 ssh_access
```

Создание VM с именем testing_config из образа:

```
openstack server create --image cirros-0.4.0-x86_64 --flavor
t2.micro --security-group ssh_access --key-name undercloud_key --
network internal --wait testing_config
```

Назначение плавающего IP адреса VM:

```
openstack server add floating ip testing_config $(openstack
floating ip create external -c id -f value)
```

2.3.5. Добавление новых узлов

Для добавления нового узла зарегистрировать и выполнить интроспекцию новых узлов так же, как это производилось при первоначальном развертывании облака.

Затем увеличить число вычислительных узлов в файле конфигурации (параметр ComputeCount или ComputeInstanceCount в случае развертывания с поддержкой высокой доступности).

После чего запустить скрипт обновления развертывания облака.

2.3.6. Замена вычислительных узлов

Прежде чем удалять вычислительный узел или узел хранения убедиться, что он не используется.

Отключение вычислительного узла

Процесс отключения вычислительного узла означает перенос с него рабочей нагрузки для того, чтобы он мог быть отключен без ущерба для доступности VM пользователей. Эта процедура может выполняться при перезагрузке вычислительного узла для обеспечения обновлений пакетов (например, после обновления ядра), при замене оборудования вычислительного узла, настройке ключей. Позволяет консолидировать рабочую нагрузку на меньшее количество машин при уменьшении переполнения;

Удаление определенных узлов из overcloud происходит с помощью команды:

```
openstack overcloud node delete --stack overcloud --templates
[директория с шаблонами] <список идентификаторов>
```

Для просмотра списка идентификаторов используется команда:

```
openstack baremetal node list
```

3. Эксплуатация облачной среды

3.1. Работа в среде управления VM

3.1.1. Вход в панель управления

Панель управления устанавливается на узле контроллера.

Оператор облака указывает имя хост-узла или общедоступный IP-адрес, с которого можно получить доступ к панели управления, а также имя пользователя и пароль. Если облако поддерживает многодоменную модель необходимо запросить доменное имя.

Открыть веб-браузер с включенными JavaScript и cookies.

Примечание. Чтобы использовать клиент Virtual Network Computing (VNC) для панели мониторинга, браузер должен поддерживать HTML5 Canvas и HTML5 WebSockets. Клиент VNC основан на noVNC. Дополнительные сведения noVNC: HTML5 VNC клиент. Список разрешенных браузеров в разделе поддержка браузеров.

В адресной строке ввести имя хост-узла или IP-адрес для панели управления, например, <https://ipAddressOrHostName/>.

Примечание. Если при первой попытке доступа к URL-адресу появляется

предупреждение сертификата безопасности, используется самоподписанный сертификат, который по умолчанию не считается надежным. Проверить сертификат или добавить исключение в браузер, чтобы обойти предупреждение.

На странице входа ввести имя пользователя и пароль и нажать кнопку [Вход]. Если облако поддерживает многодоменную модель ввести доменное имя.

Имя пользователя отображается верхней части окна.

Видимые вкладки и функции на панели управления зависят от прав доступа или ролей пользователя, с которыми выполнен вход в систему.

Если вход в систему выполнен как конечный пользователь, отображаются вкладки «Проект» («OpenStack – Проект») и «Аутентификация и авторизация» («OpenStack – Аутентификация и авторизация»).

Если вход в систему как администратор, отображаются вкладки: «Проект» («OpenStack – Проект»), Администратор («OpenStack – Администратор») и «Аутентификация и авторизация» («OpenStack – Аутентификация и авторизация»).

3.1.2. Панель управления «OpenStack» – вкладка «Проект»

Проекты (рис. 1) – это организационные единицы в облаке, которые также называются арендаторами или учетными записями. Каждый пользователь является участником одного или нескольких проектов. В рамках проекта пользователь создает экземпляры ВМ и управляет ими.

Во вкладке «Проект» можно просматривать ресурсы в выбранном проекте и управлять ими, включая экземпляры ВМ и образы. Проект выбирается с помощью выпадающего меню в верхнем левом углу. Если облако поддерживает многодоменную модель, в этом меню также можно выбрать домен.

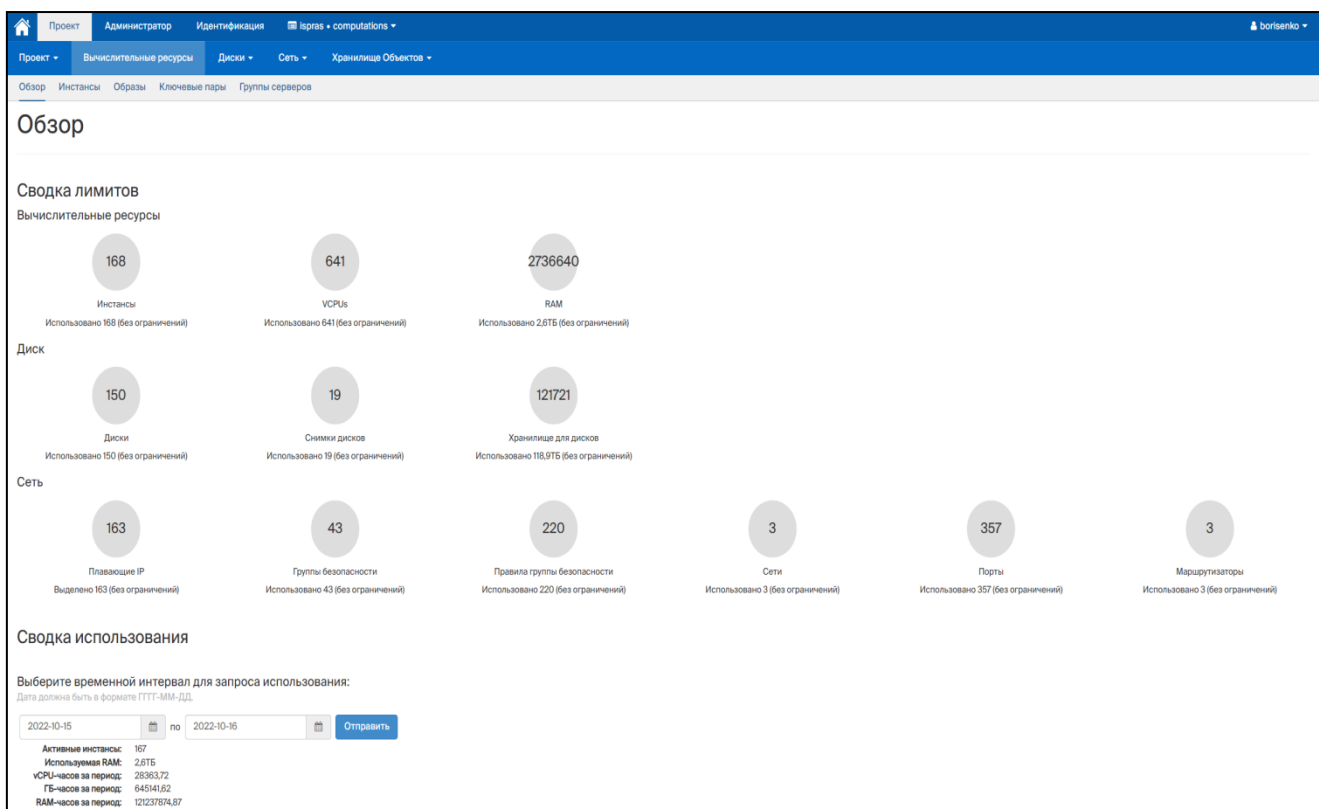


Рис. 1. Вкладка «Проект»

Во вкладке «Проект» доступ к API «Просмотр конечных точек API».

Вкладка «Служба вычислительных ресурсов»:

- обзор: просмотр отчетов по проекту»
 - экземпляры VM: просмотр, запуск, создание снимка состояния, остановка, установка на паузу или перезагрузка экземпляров VM или подключение к ним через VNC»
 - образы: просмотр образов и снимков состояния экземпляров VM, созданных пользователями проекта, а также любых общедоступных образов. Создание, редактирование и удаление образов, а также запуск экземпляров VM из образов и снимков состояния;
 - пары ключей: просмотр, создание, редактирование, импорт и удаление пар ключей.
- Вкладка «Том»:
- тома: просмотр, создание, редактирование и удаление томов;
 - резервные копии: просмотр, создание, редактирование и удаление резервных копий;
 - снимки состояния: просмотр, создание, редактирование и удаление снимков состояния ТОМОВ.

– группы устойчивости: просмотр, создание, редактирование и удаление групп устойчивости;

– снимки состояния групп устойчивости: просмотр, создание, редактирование и удаление снимков состояния групп устойчивости.

Вкладка «Сеть»:

– топология сети: просмотр топологии сети;

– сети: поздание общедоступных и частных сетей и управление ими;

– маршрутизаторы: поздание и управление маршрутизаторами;

– группы безопасности: просмотр, создание, изменение и удаление групп безопасности и правил групп безопасности;

– плавающие IP-адреса: присвоение IP-адреса или освобождение его из проекта.

Вкладка «Хранилище объектов»:

– контейнеры: создание контейнеров и объектов и управление ими.

3.1.3. Панель управления «OpenStack» – вкладка «Администратор»

Пользователи с административным доступом могут использовать вкладку «Администратор» (рис. 2) для просмотра использования и управления экземплярами ВМ, их типами, томами, образами, сетями и т.д.

The screenshot shows the OpenStack Administrator interface. At the top, there are navigation tabs for 'Проект', 'Администратор', 'Идентификация', and 'Игра + computations'. Below the navigation, there are sub-tabs for 'Вычислительные ресурсы', 'Диск', 'Сеть', and 'Система'. The main content area is titled 'Обзор' (Overview) and contains a 'Сводка использования' (Usage Summary) section. This section allows users to select a time interval for the usage report, with a dropdown menu showing '2022-10-15' and '2022-10-16'. Below the date selector, there are statistics for 'Активные экземпляры: 444', 'Используемая RAM: 515', 'VCPU-часов за период: 69495,97', 'ГБ-часов за период: 221768,62', and 'RAM-часов за период: 234702515,80'. A 'Загрузить сводку в CSV' button is also present. Below the summary is a table titled 'Использование' (Usage) with 13 columns: Project Name, VCPUs, Disk, RAM, VCPU Hours, Disk GB Hours, and Memory MB Hours. The table lists various project names and their corresponding resource usage metrics.

Project Name	VCPUs	Disk	RAM	VCPU Hours	Disk GB Hours	Memory MB Hours
1c1ed7f53be42329319df40e1ba5c15 (Удалено)	128	20,5ТБ	512ГБ	5676,99	931380,78	23252941,33
minorearth	2	50ГБ	8ГБ	88,70	2217,57	363327,21
outlanders	42	1,4ТБ	166ГБ	1862,76	64309,63	7539039,57
46234ce1f334b64935757acf5dc008f (Удалено)	16	100ГБ	64ГБ	709,62	4435,16	28066167,67
5029fde662842b98e46253c9070d61dd (Удалено)	120	2,9ТБ	240ГБ	5322,38	133054,40	10899816,25
computations	640	14,2ТБ	2,8ТБ	28384,94	645624,29	121328579,63
cuda	65	1,1ТБ	121ГБ	2882,85	50117,6	5495324,03
b71e624e352e46879b4ed9f1f6759dc (Удалено)	2	10ГБ	1ГБ	88,70	443,51	45415,90
bd1b64848ba14718f9f053b716c1ee (Удалено)	5	210ГБ	9ГБ	221,76	9313,81	408743,11
redsky	14	400ГБ	27ГБ	620,92	1740,59	1226229,33
sandbox	950	5,4ТБ	863ГБ	15521,24	246354,67	39190291,95

Рис. 2. Вкладка «Администратор»

Во вкладке «Администратор» можно получить доступ к следующим категориям для выполнения следующих задач:

Вкладка «Обзор» – просмотр основных отчетов.

Вкладка «Служба вычислительных ресурсов»:

- гипервизоры: просмотр сводной статистики гипервизора;
- агрегаты хостов: просмотр, создание и редактирование агрегатов хост-узлов.

Просмотр списка зон доступности;

– экземпляры VM: просмотр, приостановка, возобновление, установка в режим ожидания, перенос, перезагрузка всей системы или ее части, а также удаление запущенных экземпляров VM, принадлежащих пользователям некоторых (но не всех) проектов. Кроме того, просмотр журнала экземпляра VM или получение доступа к экземпляру VM через VNC;

– типы экземпляров VM: просмотр, создание, редактирование, просмотр дополнительных параметров и удаление типов экземпляров VM. Тип экземпляра VM – это размер экземпляра;

– образы: Просмотр, создание, изменение свойств и удаление пользовательских образов.

Вкладка «Том»:

- тома: просмотр, создание, удаление томов и управление ими;
- снимки состояния: просмотр, управление и удаление снимков состояния томов;
- типы томов: просмотр, создание, управление и удаление типов томов.

Вкладка «Сеть»:

- сети: просмотр, создание, изменение свойств и удаление сетей;
- маршрутизаторы: просмотр, создание, изменение свойств и удаление маршрутизаторов;
- плавающие IP-адреса: присвоение IP-адреса проекту или его освобождение.

Вкладка «Система»:

– по умолчанию: просмотр значений квот по умолчанию. Квоты жестко запрограммированы в службе вычислительных ресурсов OpenStack Compute и определяют максимально допустимый размер и количество ресурсов;

– определения метаданных: импорт пространства имен и просмотр метаданных;

– сведения о системе: для просмотра служебной информации использовать вкладки:

- службы: просмотр списка служб;
- службы вычислительных ресурсов: просмотр списка всех служб вычислительных ресурсов;

- службы блочных хранилищ: просмотр списка всех служб блочных хранилищ;
- сетевые агенты: просмотр сетевых агентов.

3.1.4. Панель управления «OpenStack» – вкладка «Аутентификация и авторизация»

На рис. 3 приведена вкладка «Аутентификация и авторизация».

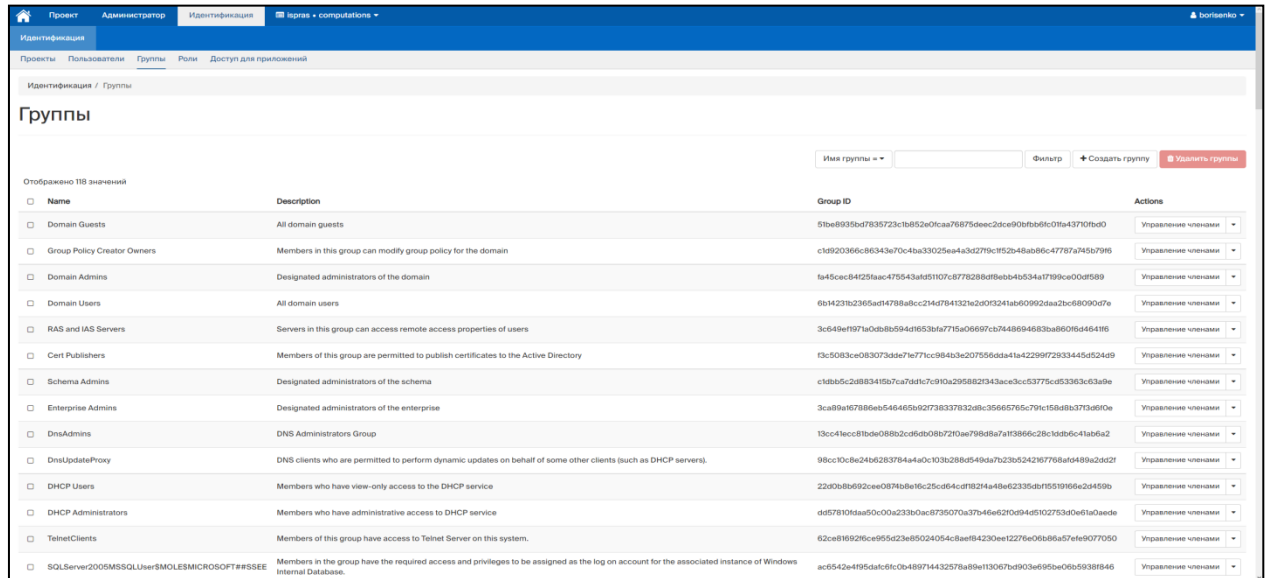


Рис. 3. Вкладка «Аутентификация и авторизация»

Во вкладке доступны:

- проекты: просмотр, создание, назначение пользователей, удаление пользователей и удаление проектов;
- пользователи: просмотр, создание, включение, отключение и удаление пользователей.

3.1.5. Панель управления «OpenStack» – вкладка «Настройки»

На рис. 4 приведена вкладка «Настройки».

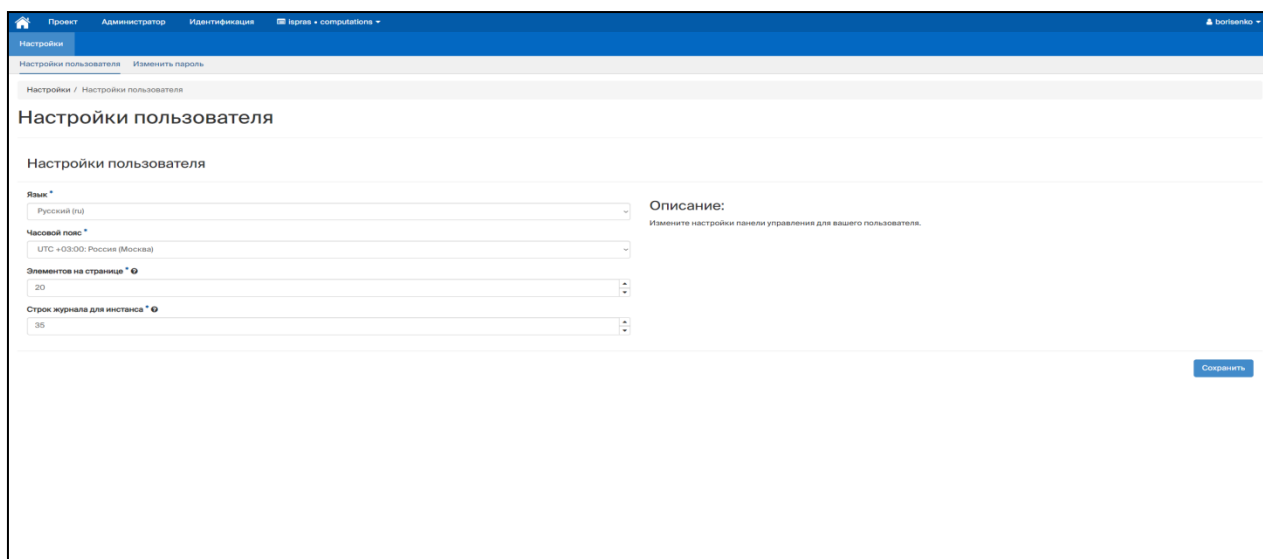


Рис. 4. Вкладка «Настройки»

Нажать кнопку [Настройки] из выпадающего меню пользователя в правом верхнем углу любой страницы, станет доступной вкладка «Настройки», в которой:

- пользовательские настройки: просмотр и управление настройками панели управления;
- изменение пароля: изменение пароля пользователя.

3.2. Загрузка образов и управление ими

Образ VM представляет собой один файл, содержащий виртуальный диск с установленной на нем загрузочной операционной системой (ОС). Образы используются для создания экземпляров VM в облаке. Сведения о создании файлов образов приведены в руководстве по созданию образов виртуальных машин OpenStack.

В зависимости от роли может быть разрешена загрузка образов VM и управление ими. Операторы могут ограничить доступ пользователей к загрузке образов и управлению ими, разрешив его только администраторам или операторам облака. Если есть соответствующие права возможно использовать панель управления для загрузки и управления образами в проекте администратора.

Примечание. Для управления образами можно также использовать клиенты командной строки `openstack` и `glance`, или службу образов.

3.2.1. Загрузка образа

Выполнить для загрузки образа в проект:

- войти в панель управления;
- выбрать соответствующий проект из выпадающего меню в левом верхнем углу;

- во вкладке «Проект» открыть вкладку службы вычислительных ресурсов и выбрать категорию «Образ»;
- выберите опцию «Создать образ».

Откроется диалоговое окно «Создать образ» (рис. 5).

Рис. 5. Панель управления «Создать образ»

Ввести следующие значения:

- имя образа – имя для образа;
- описание образа – краткое описание образа;
- источник образа – выбрать источник образа из выпадающего списка. Можно выбрать опцию «Расположение образа» или «Файл образа»;
- расположение образа или файл образа – в зависимости от выбранного источника образа можно либо ввести URL-адрес образа в поле расположение образа, либо найти файл образа в файловой системе (ФС) и добавить его;

- формат – выбрать формат образа (например, QCOW2);
- архитектура – указать архитектуру. Например, i386 для 32-разрядной архитектуры или x86_64 для 64-разрядной архитектуры;
- минимальный объем диска (Гб) – оставить это поле пустым;
- минимальный объем оперативной памяти (ОП) (Мб) – оставить это поле пустым;
- скопируйте данные – указать этот параметр для копирования данных образа в Службу образов;
- видимость – разрешение на доступ к образу. Общедоступный или частный;
- защищенный – установить этот флаг, чтобы удалить образ могли только пользователи с соответствующим разрешением. Да или нет;
- метаданные образа – указать этот параметр для добавления метаданных ресурса. Каталог метаданных glance содержит список определений метаданных образов.

Примечание. Не все поставщики услуг облачных сервисов дают доступ к этой функции.

Выбрать опцию «Создать образ». Образ отправляется в очередь для загрузки.

3.2.2. Обновление образа

Для обновления существующего образа выполнить:

- войти в панель управления;
- выбрать соответствующий проект из выпадающего меню в левом верхнем углу;
- выбрать образ, который нужно изменить;
- в столбце Действия нажать кнопку [Меню] и выбрать пункт «Редактировать образ из списка»;

В диалоговом окне «Редактирование образа» можно выполнять различные действия. Например:

- изменить имя образа;
- изменить описание образа;
- изменить формат образа;
- изменить минимальный объем диска для образа;
- изменить минимальный объем ОП для образа;
- поставив отметку Public сделать образ общедоступным.
- поставив отметку private сделать образ частным;

- изменить метаданные образа.
- Выбрать опцию «Изменить образ».

3.2.3. Удаление образа

Удаление образов является окончательным и не может быть отменено. Только пользователи с соответствующим разрешением могут удалять образы:

- войти в панель управления;
- выбрать соответствующий проект из выпадающего меню в левом верхнем углу;
- во вкладке «Проект» открыть вкладку службы вычислительных ресурсов и выбрать категорию «Образ»;
- выбрать образы, которые необходимо удалить;
- выбрать опцию «Удалить образы».

Для подтверждения удаления в диалоговом окне «Подтверждение удаления образов» нажать [Удалить образы].

3.3. Настройка доступа и безопасности для экземпляров VM

Перед запуском экземпляра VM добавить правила группы безопасности, позволяющие пользователям выполнять команду `ping` и использовать протокол SSH для подключения к экземпляру VM.

Группы безопасности – это наборы правил IP-фильтра, которые определяют доступ к сети и применяются ко всем экземплярам VM в рамках проекта. Для этого либо добавить правила в группу безопасности по умолчанию «Добавить правило в группу безопасности по умолчанию», либо добавить новую группу безопасности с правилами.

Пары ключей – это учетные данные SSH, которые внедряются в экземпляр VM при его запуске. Чтобы осуществить внедрение пары ключей, образ, на котором основан экземпляр VM, должен содержать пакет `cloud-init`. Каждый проект должен иметь минимум одну пару ключей.

Если создана пара ключей с помощью внешних инструментов, можно импортировать ее в OpenStack. Пара ключей может использоваться для нескольких экземпляров VM, принадлежащих проекту.

Примечание. Пара ключей принадлежит отдельному пользователю, а не проекту. Для совместного использования пары ключей несколькими пользователями, каждый из них должен импортировать эту пару ключей.

Когда экземпляр VM создается в OpenStack, ему автоматически назначается

фиксированный IP-адрес в сети, которой назначен экземпляр. Этот IP-адрес имеет постоянную связь с экземпляром VM, пока экземпляр не будет завершен. В дополнение к фиксированному IP-адресу, экземпляру также может быть присвоен плавающий IP-адрес. В отличие от фиксированных IP-адресов, плавающие IP-адреса могут быть изменены в любое время, независимо от состояния задействованных экземпляров VM.

3.3.1. Добавление правила в группу безопасности по умолчанию

Эта процедура позволяет протоколам SSH и ICMP (ping) осуществлять доступ к экземплярам VM. Правила применяются ко всем экземплярам VM в рамках данного проекта и должны быть установлены для каждого проекта, если нет оснований запрещать доступ SSH или ICMP к экземплярам VM.

Эта процедура может быть скорректирована по мере необходимости для добавления дополнительных правил группы безопасности в проект, если они требуются в облаке.

Примечание. При добавлении правила указать протокол, используемый в порте назначения или порте источника.

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу. Во вкладке «Проект» открыть вкладку «Сеть». Во вкладке «Группы безопасности» отображаются группы безопасности, доступные для данного проекта.

Выбрать группу безопасности по умолчанию и перейти в «Управление правилами».

Выбрать «Добавить правило» для разрешения доступ по SSH.

В диалоговом окне «Добавление правила» ввести следующие значения:

Rule: SSH

Remote: CIDR

CIDR: 0.0.0.0/0

Примечание. Чтобы принимать запросы от определенного диапазона IP-адресов указать блок этих IP-адресов в поле CIDR.

Нажать [Добавить] – теперь экземпляры VM получают SSH-порт 22, открытый для запросов с любого IP-адреса.

Для добавления правила ICMP выбрать опцию «Добавить правило».

В диалоговом окне Добавление правила ввести следующие значения:

Rule: All ICMP

```
Direction: Ingress
```

```
Remote: CIDR
```

```
CIDR: 0.0.0.0/0
```

Нажать [Добавить]. Теперь экземпляры VM смогут принимать все входящие пакеты ICMP.

3.3.2. Добавление пары ключей

Для каждого проекта необходимо создать минимум одну пару ключей, выполнив:

- войти в панель управления;
- выбрать соответствующий проект из выпадающего меню в левом верхнем углу;
- во вкладке «Проект» открыть вкладку «Служба вычислительных ресурсов»;
- перейдите во вкладку «Пара ключей», на которой отображаются пары ключей, доступные для данного проекта;
- выбрать опцию «Создать пару ключей».

В диалоговом окне «Создание пары ключей» ввести имя пары ключей и нажать [Создать пару ключей]. Приватный ключ будет загружен автоматически.

Для ограничения его разрешения (чтение, внесения записи в файл) выполнить команду:

```
$ chmod 0600 yourPrivateKey.pem
```

Примечание. Если выполнять через панель управления на компьютере с установленной ОС Windows, использовать PuTTYgen для загрузки файла *.pem, конвертировать и сохранить его как *.ppk. Для получения дополнительной информации см. веб-страницу WinSCP для PuTTYgen.

Чтобы сделать пару ключей известной для SSH, выполните команду:

```
ssh-add
```

```
$ ssh-add yourPrivateKey.pem
```

3.3.3. Импорт пары ключей

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Служба вычислительных ресурсов.»

Перейти во вкладку «Пара ключей», на которой отображаются пары ключей, доступные для данного проекта.

Выбрать опцию «Импортировать пару ключей».

В диалоговом окне «Импорт пары ключей» ввести имя пары ключей, скопировать открытый ключ в поле «Открытый ключ» и нажать [Импорт пары ключей].

База данных службы вычислительных ресурсов регистрирует открытый ключ этой пары ключей.

Список пар ключей отображается в Панели управления во вкладке «Пары ключей».

3.3.4. Присвоение экземпляру VM плавающего IP-адреса

Когда экземпляр VM создается в OpenStack, ему автоматически назначается фиксированный IP-адрес в сети, которой назначен экземпляр. Этот IP-адрес имеет постоянную связь с экземпляром VM, пока экземпляр не будет завершен.

В дополнение к фиксированному IP-адресу, экземпляру также может быть присвоен плавающий IP-адрес. В отличие от фиксированных IP-адресов, плавающие IP-адреса можно изменять в любое время, независимо от состояния задействованных экземпляров VM. Эта процедура детализирует резервирование плавающего IP-адреса из существующего пула адресов и связывание этого адреса с конкретным экземпляром VM.

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Сеть.»

Перейти во вкладку «Плавающие IP-адреса», на которой отображаются плавающие IP-адреса, присвоенные экземплярам VM.

Выбрать опцию «Присвоить проекту IP-адрес».

Выбрать пул, из которого нужно выбрать IP-адрес.

Нажать [Присвоить IP].

В списке «Плавающие IP-адреса» выбрать опцию «Связать».

В диалоговом окне «Управление назначением плавающих IP-адресов» выбрать следующие параметры:

– поле IP-адрес заполняется автоматически, но можно добавить новый IP-адрес, нажав кнопку [+];

– в поле «Порт для связи» выбрать порт из списка.

В списке отображаются все экземпляры VM с фиксированными IP-адресами.

Выберите опцию «Связать».

Примечания:

1. Для удаления связи IP-адреса с экземпляром VM выбрать «Отмена связи».

2. Чтобы вернуть плавающий IP-адрес обратно в пул плавающих IP-адресов, выбрать параметр «Освободить плавающий IP» в столбце «Действия».

3.3.5. Запуск экземпляров VM и управление ими

Экземпляры VM – это VM, работающие в облаке. Экземпляр VM можно запустить из следующих источников:

- образы, загруженные в Службу образов;
- образ, скопированный на постоянный том. Экземпляр VM запускается с тома, который предоставляется API cinder-volume через iSCSI;
- снимок состояния экземпляра VM.

3.3.6. Запуск экземпляра VM

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку службы вычислительных ресурсов и выбрать категорию «Экземпляры VM».

Панель управления отображает экземпляры VM в виде имени VM, ее приватного IP, плавающего IP, размера, статуса, текущего задания, состояния питания и так далее.

Выбрать «Запустить экземпляр VM». В диалоговом окне Запуск экземпляра VM ввести следующие значения:

- вкладка «Сведения»;
- имя экземпляра VM;
- назначить имя VM.

Примечание. Имя, которое назначено здесь, становится изначальным `hostname server`. Если имя длиннее 63-х символов, служба вычислительных ресурсов автоматически обрезает его, чтобы обеспечить корректную работу `dnsmasq`.

Если после создания сервера изменить его имя в API или изменить имя хоста напрямую, на панели управления имена обновлены не будут.

Создаваемые имена серверов не гарантированно уникальны, поэтому может быть два экземпляра VM с одинаковым именем хоста.

Описание – можно снабдить VM кратким описанием.

Зона доступности – по умолчанию это значение устанавливается в зону доступности, заданную поставщиком услуг облачного сервиса (например, `us-west` или `arac-south`). Для некоторых случаев значением может быть `nova`.

Количество – чтобы запустить несколько экземпляров VM, ввести значение

больше 1. Значение по умолчанию – 1.

Вкладка «Источник» – источник загрузки экземпляра VM.

Можно выбрать следующие опции:

Загрузка из образа – при выборе этого параметра отображается новое поле Имени образа. Образ выбирается из списка.

Загрузка из снимка состояния – при выборе этого параметра отображается новое поле Снимка состояния экземпляра VM. Снимок выбирается из списка.

Загрузка из Тома – при выборе этого параметра отображается новое поле Тома. Том выбирается из списка.

Загрузка из образа (создает новый том) – с помощью этой опции производится загрузка из образа и создается том, с указанием размера и имени устройства для тома. Выбрать опцию «Удалить том» в меню «Удаление экземпляра VM», для удаления тома при удалении экземпляра VM.

Загрузка из снимка состояния тома (создает новый том) – с помощью этой опции можно произвести загрузку из снимка состояния тома и создать новый том, выбрав Снимок состояния тома из списка и добавив имя устройства для своего тома. Выбрать опцию «Удалить том» в меню «Удаление экземпляра VM», для удаления тома при удалении экземпляра VM.

Имя образа – это поле изменяется в зависимости от Вашего предыдущего выбора. Если выбран запуск экземпляра VM с помощью образа, отобразится поле Имя образа. Выбрать имя образа из выпадающего списка.

Снимок состояния экземпляра VM – это поле изменяется в зависимости от предыдущего выбора. Если был выбран запуск экземпляра VM с помощью снимка состояния, отобразится поле Снимок состояния экземпляра VM. Выбрать имя снимка из выпадающего списка.

Том – это поле изменяется в зависимости от предыдущего выбора. Если был выбран запуск экземпляра VM с помощью тома, отобразится поле «Том». Выбрать имя тома из выпадающего списка. Для удаления тома при удалении экземпляра VM, установить флаг «Удалить том» в меню «Удаление экземпляра VM».

Во вкладке «Тип экземпляра VM» выбрать тип экземпляра VM и указать размер экземпляра VM для запуска.

Примечание. Тип инстанса выбирается на основе размера образа, выбранного для запуска экземпляра VM. Например, если при создании образа в поле Минимальный объем ОП (Мб) введено значение 2048, то при выборе образа типом инстанса по умолчанию является m1.small.

Во вкладке «Сети» выбрать «Выбранные сети» для добавления сети к экземпляру VM и нажать кнопку [+] в поле «Доступно».

Во вкладке «Сетевые порты» выбрать «Порты» и активируйте порты, которые необходимо назначить для экземпляра VM.

Во вкладке «Группы безопасности» выбрать «Группы безопасности» и активировать группы безопасности, которые необходимо назначить для экземпляра VM.

Группы безопасности – это своего рода облачный брандмауэр, который определяет, какой входящий сетевой трафик передается экземплярам VM.

Если не были созданы группы безопасности, можно назначить экземпляру VM только группу безопасности по умолчанию.

Во вкладке «Пара ключей» выбрать «Пара ключей» и указать пару ключей.

Если образ использует статический пароль администратора или набор статических ключей (ни один, из которых не рекомендован), то для запуска экземпляра VM не требуется указывать пару ключей.

Во вкладке «Конфигурация» выбрать исходный код скрипта настройки и указать скрипт настройки, который запустится после старта экземпляра VM.

Во вкладке «Метаданные» выбрать «Доступные метаданные» и добавить элементы метаданных в экземпляр VM.

Выбрать «Запустить экземпляр VM». Экземпляр запускается на вычислительном узле в облаке.

Примечание. Если Вы не предоставили пару ключей, группы безопасности или правила, пользователи могут получить доступ к экземпляру VM только из облака через VNC. Даже проверка экземпляра с помощью ping-запросов невозможна без настроенного правила ICMP.

Также можно запустить экземпляр VM из категорий «Образа» или «Тома» при запуске экземпляра из образа или тома соответственно.

При запуске экземпляра VM из образа OpenStack создает локальную копию образа на вычислительном узле, где запускается экземпляр VM.

Дополнительные сведения о создании образов в разделе Создание образов вручную в Руководстве по работе с образами VM OpenStack.

При запуске экземпляра VM из тома выполнить следующие действия:

- Чтобы выбрать том для запуска, запустите экземпляр VM из произвольного образа на томе. Выбранный произвольный образ не загружается. Вместо этого он заменяется образом из тома, который Вы выберете далее.

- для загрузки образа Xen с тома запускаемый образ должен быть того же ти-

па, полностью виртуализированный или паравиртуализированный, как и образ на томе;

- выбрать том или снимок состояния тома для загрузки. Ввести имя устройства. Ввести vda для образов KVM или xvda для образов Xen.

Примечание. При запуске QEMU без поддержки аппаратной виртуализации установить `cpu_mode= "none"` вместе с `virt_type=qemu` в `/etc/nova/nova-compute.conf` для решения следующей ошибки:

```
libvirtError: unsupported configuration: CPU mode 'host-model'
for ``x86_64`` qemu domain on ``x86_64`` host is not supported
by hypervisor
```

3.3.7. Подключение к экземпляру VM с помощью SSH

Чтобы использовать SSH для подключения к нужному экземпляру VM, использовать скачанный файл с парой SSH-ключей.

Примечание. Имя пользователя - `ubuntu` для образов облака Ubuntu на TryStack.

Скопировать IP-адрес для нужного экземпляра VM.

Использовать команду `ssh` для безопасного подключения к экземпляру.

Например:

```
$ ssh -i MyKey.pem ubuntu@10.0.0.2
```

В командной строке ввести `да`.

Также возможно подключить SSH к экземпляру VM без пары SSH-ключей, если администратор разрешил ввод пароля суперпользователя. Дополнительные сведения по вводу пароля суперпользователя в разделе Введение пароля администратора в Руководстве администратора OpenStack.

3.3.8. Отслеживание использования экземпляров VM

Возможно отслеживание использования экземпляров VM для каждого проекта. Можно отслеживать затраты в месяц по счетчикам, таким как количество vCPUs, дисков, ОП и времени работы для всех ваших экземпляров VM.

Войти в панель управления.

Выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку службы вычислительных ресурсов и выбрать категорию «Обзор».

Чтобы запросить статистику использования экземпляра VM за месяц, выбрать месяц и нажать кнопку [Отправить].

Чтобы загрузить сводную статистику, выбрать «Загрузить CSV-статистику».

3.3.9. Создание снимка состояния экземпляра VM

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку службы вычислительных ресурсов и выбрать категорию «Экземпляры VM».

Выбрать экземпляр VM, с которого будет создан снимок состояния.

В столбце действий выбрать «Создать снимок».

В диалоговом окне «Создание снимка состояния» ввести имя снимка и нажать кнопку [Создать снимок].

Снимок состояния отображается в категории «Образы».

Для запуска экземпляра VM из снимка состояния выбрать снимок и нажать кнопку [Запустить].

3.3.10. Управление экземпляром VM

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку службы вычислительных ресурсов и выберите категорию «Экземпляры VM».

Выбрать экземпляр VM.

В списке меню в столбце действий выбрать состояние.

Можно изменить размер экземпляра VM или перестроить его. Также просматривать журнал консоли экземпляра и редактировать экземпляр или группы безопасности. В зависимости от текущего состояния экземпляра VM его можно приостановить, возобновить, поставить в режим ожидания, осуществить мягкую или жесткую перезагрузку или удалить его.

3.4. Создание сетей и управление ими

Служба управления сетью OpenStack предоставляет масштабируемую систему для управления сетевым подключением в рамках развертывания облака OpenStack. Она может легко и быстро реагировать на изменение потребностей сети (например, создавая и назначая новые IP-адреса).

Сетевое взаимодействие в OpenStack комплексное. В этом разделе приведены основные инструкции по созданию сети и маршрутизатора. Подробные сведения об управлении сетями в Руководстве по управлению сетями OpenStack.

3.4.1. Создание сети

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть «Сеть» и выбрать категорию Сети.

Выбрать опцию «Создать сеть».

В диалоговом окне «Создать сеть» ввести следующие значения:

- вкладка «Сеть» – имя сети: указать имя для идентификации сети:
 - общий доступ: открыть доступ к сети для других проектов. Пользователи, не являющиеся администраторами, не могут настраивать общий доступ;
 - статус администратора: статус, позволяющий запускать сеть;
 - создание подсети: установить флаг для создания подсети. Не нужно указывать подсеть при создании сети, но если не указать её, подключение сети к экземпляру VM будет невозможно;
- вкладка «Подсети» – имя подсети: укажите имя подсети:
 - адрес сети: указать IP-адрес для подсети;
 - версия IP: выбрать IPv4 или IPv6;
 - IP шлюза: указать IP-адрес для конкретного шлюза. Этот параметр является необязательным;
 - отключить шлюз: установите флаг для отключения IP-адрес шлюза;
- вкладка «Сведения о подсети»:
 - включение DHCP: установить флаг для включения DHCP;
 - пулы выделения IP-адресов: указать пулы для выделения IP-адресов;
 - DNS-серверы имен: указать имя DNS-сервера;
 - таблица маршрутизации хоста: указать таблицу маршрутизации хоста.

Выбрать опцию «Создать».

Сеть отображается во вкладке «Сети» на панели управления.

3.4.2. Создание маршрутизатора

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Сеть» и выбрать категорию «Маршрутизаторы».

Выбрать опцию «Создать маршрутизатор».

В диалоговом окне «Создание маршрутизатора» указать имя маршрутизатора и внешней сети и выбрать «Создать маршрутизатор».

Новый маршрутизатор будет отображаться во вкладке «Маршрутизаторы».

Чтобы подключить частную сеть к новому маршрутизатору, выполнить:

- во вкладке «Маршрутизаторы» выбрать имя маршрутизатора.
- на странице «Сведения о маршрутизаторе» перейти во вкладку «Интерфейсы» и выбрать опцию «Добавить интерфейс».
- в диалоговом окне «Добавление интерфейса» выбрать «Подсеть».

При необходимости задать IP-адрес интерфейса маршрутизатора для выбранной подсети в диалоговом окне «Добавление интерфейса».

Если не нужно устанавливать значение IP-адреса, то по умолчанию служба управления сетями OpenStack использует первый IP-адрес хоста в подсети.

Поля «Имя маршрутизатора» и «Идентификатор маршрутизатора» обновляются автоматически.

Выбрать опцию «Добавить Интерфейс».

Маршрутизатор создан. Новую топологию можно просмотреть во вкладке «Топология сети».

3.4.3. Создание порта

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» выбрать категорию сети.

Выбрать имя сети, в которой будет создан порт.

Перейти во вкладку «Порты» и выбрать опцию «Создать порт».

В диалоговом окне «Создание порта» указать следующие значения:

- имя: указать имя для идентификации порта;
- идентификатор устройства: закрепленный за портом идентификатор устройства;
- владелец устройства: закрепленный за портом владелец устройства;
- связанный хост: значение ID хоста, для которого выделяется порт;
- тип привязываемого виртуального сетевого адаптера: выбрать тип привязываемого виртуального сетевого адаптера (VNIC) к порту Neutron;
- выбрать опцию «Создать порт».

Новый порт будет отображаться в списке портов.

3.4.4. Создание контейнеров для объектов и управление ими

Объектное хранилище Openstack Swift используется для масштабируемого хранения данных с избыточностью на основе кластеров, состоящих из серверов об-

щедоступного класса. Это система долговременного хранения больших объемов статических данных, которые можно восстанавливать и обновлять.

Объектное хранилище OpenStack предоставляет распределенную, доступную API платформу хранения, которая может быть интегрирована непосредственно в приложение или использоваться для хранения файлов любого типа, в том числе образов VM, резервных копий, архивов или мультимедийных файлов. Панель управления OpenStack позволяет управлять только контейнерами и объектами.

В объектном хранилище OpenStack объекты хранятся в контейнерах аналогично папке Windows или каталогу файлов Linux, однако они не могут быть вложенными. Объект в OpenStack состоит из хранящегося в контейнере файла и любых сопутствующих метаданных.

3.4.5. Создание контейнера

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Хранилище объектов» и выбрать категорию «Контейнеры». Выбрать опцию «Контейнер».

В диалоговом окне «Создание контейнера» ввести имя контейнера и нажать кнопку [Создать].

Примечание. Для удаления контейнера перейти в меню «Дополнительно» и выбрать опцию «Удалить контейнер».

3.4.6. Загрузка объекта

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Хранилище объектов» и выбрать категорию «Контейнеры».

Выбрать контейнер, в котором необходимо сохранить объект.

Нажать кнопку [Загрузить файл].

Загрузка файла в контейнер: появится диалоговое окно <имя>. <имя> – это имя контейнера, в который загружается объект.

Ввести имя объекта.

Выбрать файл, который необходимо загрузить.

Выбрать «Загрузить файл».

Примечание. Для удаления объекта перейти в раздел «Дополнительно» и выбрать опцию «Удалить объект».

3.4.7. Управление объектом

Редактирование объекта:

- войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.
- во вкладке «Проект» открыть вкладку «Хранилище объектов» и выбрать категорию «Контейнеры»;
- выбрать контейнер, в котором сохранить объект;
- перейти в меню и выбрать опцию «Изменить» из выпадающего списка;
- откроется диалоговое окно «Изменить объект»;
- выбрать файл, который необходимо загрузить;
- выбрать опцию «Обновить объект».

Примечание. Для удаления объекта перейти в раздел «Меню» и выбрать опцию «Удалить объект».

Копирование объекта из одного контейнера в другой:

- войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу;
- во вкладке «Проект» открыть вкладку «Хранилище объектов» и выбрать категорию «Контейнеры»;
- выбрать контейнер, в котором необходимо сохранить объект;
- перейти в меню и выбрать опцию «Копировать» из выпадающего списка.

В диалоговом окне «Запуск копирования объекта» ввести значения и выбрать опцию «Копировать объект»:

- контейнер назначения: выбрать контейнер назначения из списка;
- путь: указать путь сохранения новой копии внутри выбранного контейнера;
- имя объекта назначения: ввести имя объекта в новом контейнере.

Создание объекта только для метаданных без файла:

В контейнере можно создать новый объект без файла или загрузить файл позже, когда он будет готов. Этот временный объект резервирует место для нового объекта и позволяет заранее предоставлять метаданные объекта и информацию URL для совместного использования.

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» откройте вкладку «Хранилище объектов» и выбрать категорию «Контейнеры». Выбрать контейнер, в котором необходимо сохранить объект.

Выбрать опцию «Загрузить объект».

Загрузка объекта в контейнер: откроется диалоговое окно <имя>, где <имя> – это имя контейнера, в который загружается объект.

Ввести имя объекта и выбрать опцию «Обновить объект».

Создание псевдо-папки:

Псевдо-папки похожи на папки в настольной ОС. Это виртуальные коллекции, которые группируются по общему префиксу в имени объекта.

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Хранилище объектов» и выбрать категорию «Контейнеры».

Выбрать контейнер, в котором необходимо сохранить объект.

Выбрать опцию «Создать псевдо-папку».

Появится диалоговое окно «Создать псевдо-папку в контейнере»: <имя>, где <имя> – это имя контейнера, в который загружается объект.

Ввести имя псевдо-папки.

Символ косой черты (/) используется в качестве разделителя для псевдо-папок в объектном хранилище. Выбрать опцию «Создать»

3.5. Создание томов и управление ими

Тома – это элементы блочного хранения, которые подключаются к экземплярам ВМ для постоянного хранения. В любое время возможно подключить том к работающему экземпляру ВМ или отключить том и присоединить его к другому экземпляру. Можно также создать снимок состояния из тома или удалить том. Типы томов могут только администраторы.

3.5.1. Создание тома

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» откройте вкладку «Тома» и выбрать категорию «Тома».

Выбрать опцию «Создать том».

В открывшемся диалоговом окне ввести или выбрать следующие значения:

- имя тома: указать имя для тома;
- описание: при необходимости ввести краткое описание тома;
- источник тома: выбрать одну из следующих опций:
 - нет источника, пустой том: создает пустой том. В пустом томе нет ФС или

таблицы разделов;

- снимок состояния: при выборе этого параметра отображается новое поле «Снимок состояния как источник». Можно выбрать снимок состояния из списка;

- образ: при выборе этого параметра отображается новое поле «Образ как источник». Можно выбрать образ из списка;

- том: при выборе этого параметра отображается новое поле «Том как источник». Можно выбрать том из списка. Параметры использования снимка состояния или тома как источника для тома отображаются только при наличии существующих моментальных снимков или томов;

- тип: оставить это поле пустым;

- размер (Гб): размер тома в гигабайтах (GiB);

- зона доступности: выбрать зону доступности из списка. По умолчанию это значение устанавливается в зону доступности, заданную поставщиком услуг облачного сервиса (например, us-west или aрас-south). Для некоторых случаев значением может быть nova;

- выбрать опцию «Создать том»;

- том отображается во вкладке «Тома на панели управления».

3.5.2. Подключение тома к экземпляру VM

После создания одного или нескольких томов их можно подключить к экземплярам VM. Одновременно можно подключить один том к одному экземпляру.

Войти в панель управления и выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Тома» и выбрать категорию Тома.

Выбрать том для добавления в экземпляр VM и опцию «Управление подключениями». В диалоговом окне «Управление подключениями томов» выбрать экземпляр VM. Ввести имя устройства, с которого экземпляр получает доступ к тому.

Примечание. Реальное имя устройства может отличаться от имени тома из-за настроек гипервизора.

Выбрать опцию «Подключить том».

На панели управления отобразится экземпляр VM, к которому теперь подключен том, и имя устройства.

Состояние тома можно просмотреть во вкладке «Тома» на панели управления. Том имеет статус «Доступен или «Используется».

После возможно войти в экземпляр VM и монтировать, форматировать и ис-

пользовать диск.

3.5.3. Отключение тома от экземпляра VM

Войти в панель управления выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Тома» и выбрать категорию Тома.

Выбрать том и перейти в «Управление подключениями».

Выбрать опцию «Отключить том» и подтвердите изменения. Появится сообщение о том, было ли действие выполнено успешно.

3.5.4. Создание снимка состояния с тома

Войти в панель управления выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Тома» и выбрать категорию Тома.

Выбрать том, с которого будет создан снимок состояния.

В столбце «Действия» выбрать «Создать снимок». В открывшемся диалоговом окне ввести имя снимка, его краткое описание и подтвердить изменения.

Новый снимок состояния тома будет отображаться на панели управления во вкладке «Снимки состояния тома».

3.5.5. Редактирование тома

Войти в панель управления выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Тома» и выбрать категорию Тома.

Выбрать том, который необходимо изменить.

В столбце «Действия» выбрать «Изменить том».

В диалоговом окне «Изменить том» обновить имя и описание тома и выбрать опцию «Изменить том».

Примечание. Можно расширить том с помощью опции «Расширить том» из раскрывающегося списка «Дополнительно», введя новое значение для размера тома.

3.5.6. Удаление тома

При удалении экземпляра VM данные в его подключенных томах не удаляются.

Войти в панель управления выбрать соответствующий проект из выпадающего меню в левом верхнем углу.

Во вкладке «Проект» открыть вкладку «Тома» и выбрать категорию Тома.

Установить флаги напротив томов, которые требуется удалить.

Выбрать опцию «Удалить том» и подтвердите выбор. Появится сообщение о том, было ли действие выполнено успешно.

4. Описание процессов, обеспечивающих поддержание жизненного цикла ПО

4.1 Процессы разработки и совершенствования ПО

Разработка инструментов развертывания облачной среды Асперитас ведется по методологии Agile с привлечением современных средств повышения качества кода.

1. Для хранения кода используется система контроля версий git, и изменения в основной ветке проходят инспекцию кода (code review) другими разработчиками.
2. При написании кода разработчики должны придерживаться строгих правил оформления кода; нарушение этих правил не позволит пройти этап инспекции кода.
3. Используется инструментарий, позволяющий выполнять первичную валидацию конфигурации.
4. Периодически производится проверка кода среды на предмет наличия ошибок

4.2 Поддержка пользователей ПО

Пользователи, которым достаточно для решения их задач возможностей, уже реализованных в среде анализа алгоритмов, могут приступать к работе со средой после краткого обучения, проводимого на стороне разработчика (ИСП РАН). В ходе своей работы среда Асперитас автоматически ведёт журналы действий и ошибок, которые могут быть отправлены разработчику в случае обнаружения некорректного поведения или возникновения запроса на улучшение и доработку.

Информация о сбоях в работе среды Асперитас, проблемах производительности, ошибках целевого функционала передаются пользователями среды непосредственно ответственным сотрудникам ИСП РАН, без использования публичных Интернет-ресурсов управления ошибками. Это обеспечивает должный уровень конфиденциальности для контрольных примеров, передаваемых пользователем среды в ИСП РАН для оценки и исправления программного дефекта.

Со своей стороны ИСП РАН постоянно совершенствует Асперитас, применяя в жизненном цикле разработки передовые методики. Добавление новых и улучшение

существующих алгоритмов ведется в инициативном порядке. Обновления среды Асперитас передаются пользователям среды через согласованные с ними каналы распространения обновлений.

4.3 Необходимый персонал для разработки и поддержки

Персонал должен обладать следующими навыками:

1. Опыт работы и понимание принципов работы облачных систем.
2. Опыт инсталляции, настройки и администрирования пользовательского, системного и СПО.
3. Навыки и опыт администрирования ОС на базе ядра Linux.
4. Опыт построения кластерных систем.
5. Опыт работы и понимание архитектуры распределенных файловых систем.

Для разработки и поддержки программного продукта необходима соответствующая квалификация разработчиков. Это вызвано следующими причинами:

1. Специфическая предметная область, требующая глубоких знаний одновременно в нескольких областях: устройство современной аппаратуры и операционных систем, системное администрирование, компьютерная безопасность, технологии разработки ПО.
2. Наличие среди алгоритмов, реализованных в среде развертывания, алгоритмов, впервые разработанных сотрудниками ИСП РАН.
3. Требования к производительности системы.

В силу приведенных причин коллектив разработчиков Асперитас формируется из специалистов, получивших профильное образование.

Для гарантийного обслуживания задействовано 5 программиста и научных сотрудников, для Технической поддержки задействованы 3 программиста, для модернизации программного обеспечения задействованы 10 научных сотрудников и программистов.

Адрес электронной почты, по которому можно обратиться по вопросам, связанным с облачной средой «Асперитас» — asperitas@ispras.ru.