КИБЕРПРОТЕКТ

КИБЕР Инфраструктура

Версия 5.5

Руководство по самообслуживанию

Редакция: 22.04.2024

Заявление об авторских правах

Содержание

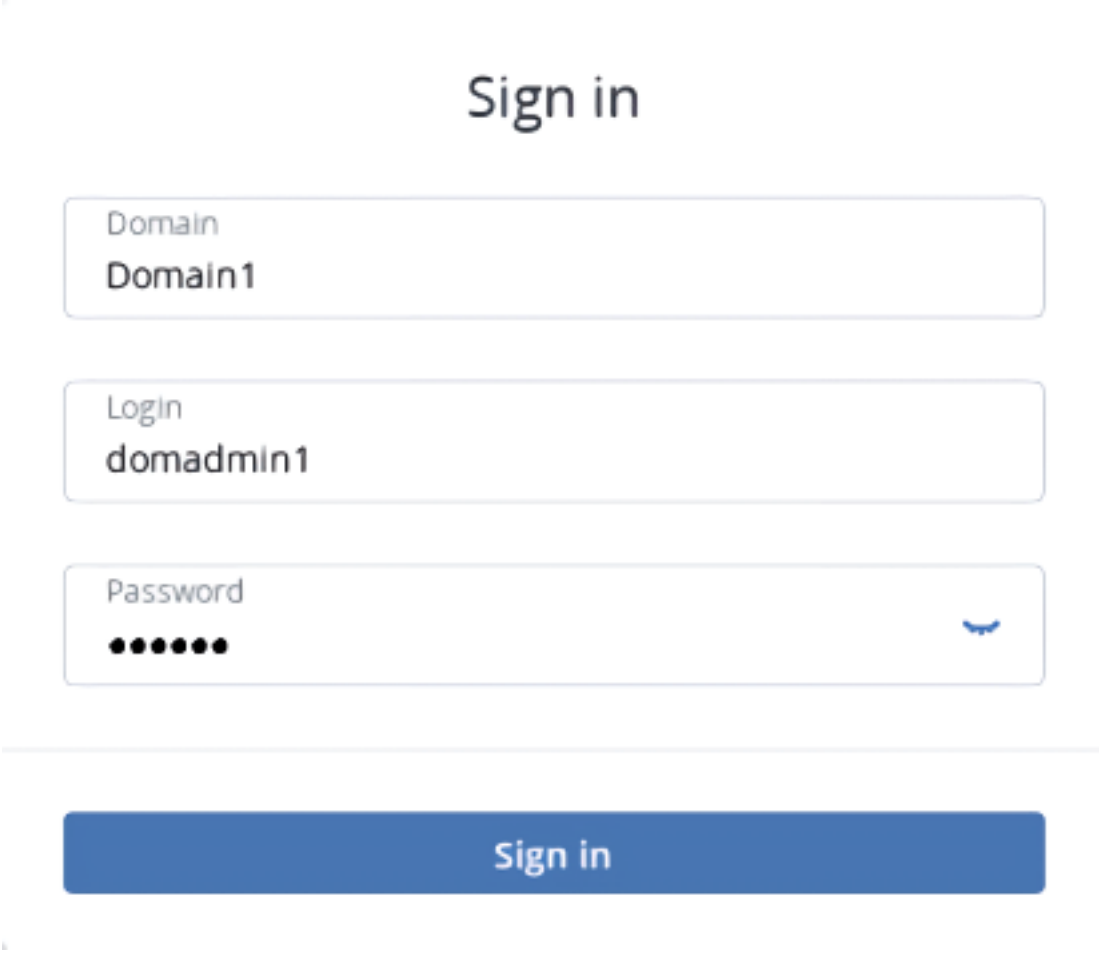
1 Об этом руководстве

Это руководство предназначено для администраторов доменов и участников проектов. В нем описывается управление вычислительными ресурсами и пользователями проекта с помощью панели самообслуживания.

2 Вход на панель самообслуживания

Как выполнить вход на панель самообслуживания

1. Откройте IP-адрес панели через порт 8800.
2. Введите доменное имя (с учетом регистра), имя пользователя и пароль. Если вы используете ссылку на панель самообслуживания для определенного домена, потребуется ввести только имя пользователя и пароль.



3 Управление уведомлениями

В центре уведомлений хранятся и отображаются уведомления о последних заданиях текущего пользователя на панели управления. Уведомления отображаются только для заданий, выполненных во время текущего пользовательского сеанса, и очищаются после выхода пользователя.

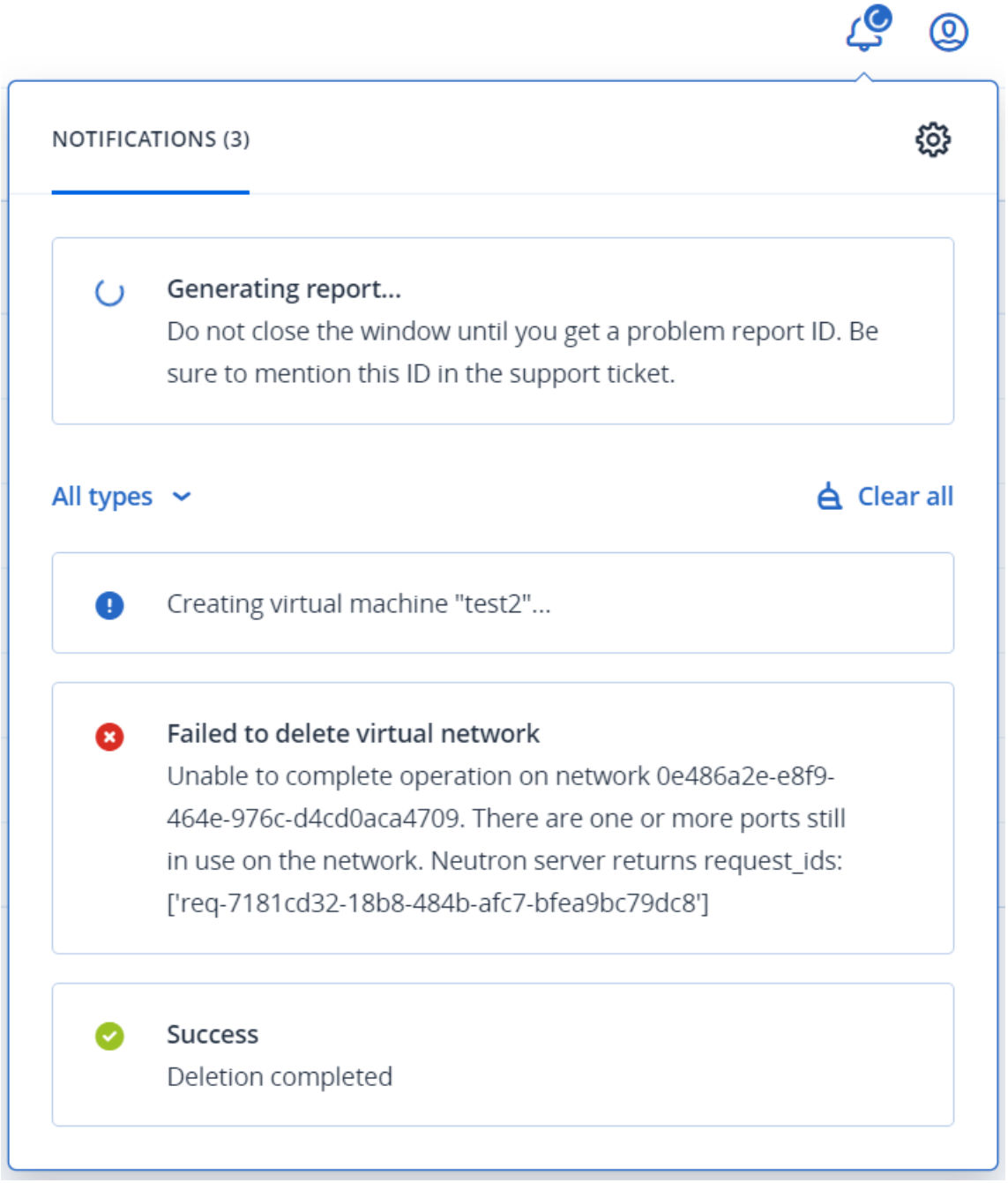
Пользователь информируется о каждом задании с помощью всплывающего уведомления в правом нижнем углу. Это же уведомление также отображается в центре уведомлений. После закрытия всплывающего окна уведомление будет доступно в центре уведомлений.

В следующей таблице описаны все поддерживаемые типы уведомлений.

Тип уведомления	Значок	Описание	Время отображения всплывающего окна	Срок хранения в центре уведомлений
Сведения		Уведомления о запуске заданий	3 секунд	10 минут
Успешно		Уведомления об успешно выполненных заданиях	3 секунд	10 минут
Error		Уведомления о заданиях, завершившихся ошибкой	10 секунд	50 минут
Выполняется		Длительные задания, такие как передача образа или создание отчета о проблеме	Время выполнения задания	Время выполнения задания

Как просмотреть уведомления

Нажмите значок колокольчика в правом верхнем углу.

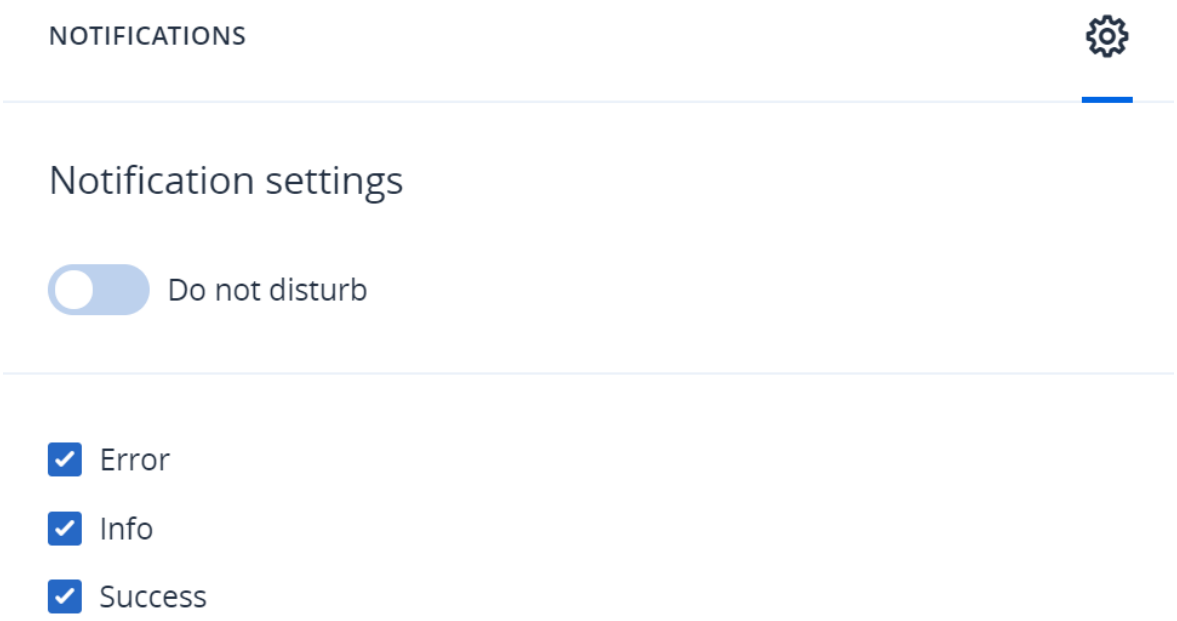


Рядом со значком колокольчика расположен счетчик уведомлений или значок загрузки, если в данный момент выполняется задание.

Как настроить уведомления

1. На любом экране щелкните по значку колокольчика в правом верхнем углу.
2. Щелкните по значку шестерни и выберите типы уведомлений, которые следует отображать в

центре уведомлений.



Как очистить уведомления

1. На любом экране щелкните по значку колокольчика в правом верхнем углу.
2. Чтобы удалить только одно уведомление, нажмите крестик рядом с ним.
3. Чтобы очистить все уведомления, нажмите **Очистить все** над списком уведомлений.

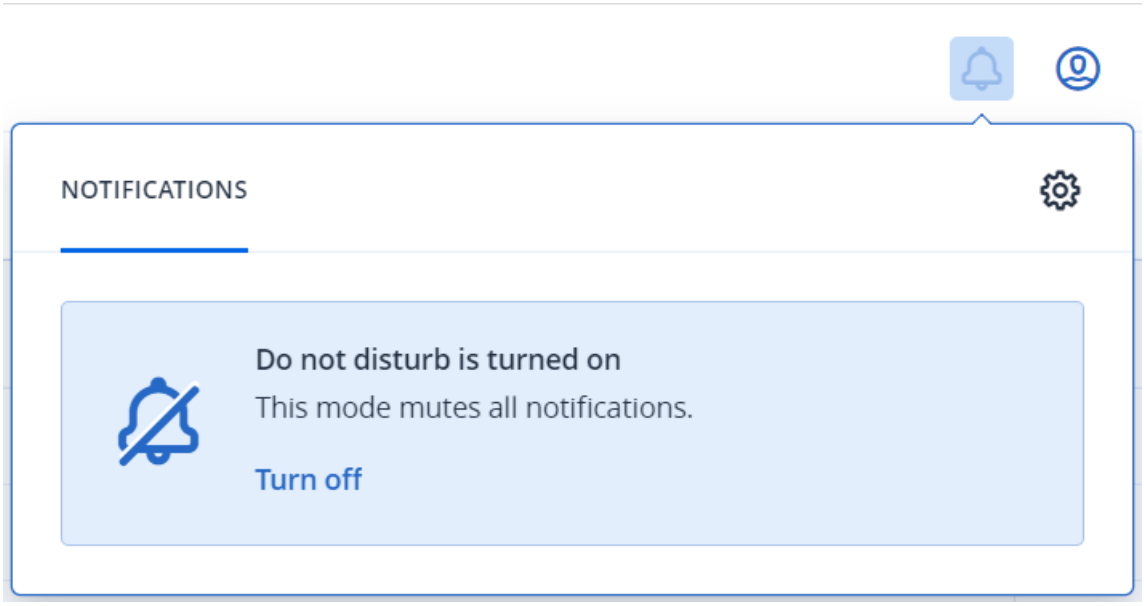
Как скрыть уведомления

1. На любом экране щелкните по значку колокольчика в правом верхнем углу.
2. Щелкните по значку шестерни и включите режим **Не беспокоить**.

Значок колокольчика станет серым, а счетчик уведомлений исчезнет. При этом последние уведомления по-прежнему будут доступны в центре уведомлений.

Как снова включить показ уведомлений

1. На любом экране щелкните по серому значку колокольчика в правом верхнем углу.
2. Нажмите **Отключить**, чтобы отключить режим **Не беспокоить**.



4 Управление пользователями и проектами

На панели самообслуживания можно создавать пользователей и назначать их на проекты внутри домена. При создании пользователя выбирается его роль. Пользователю можно назначить одну из следующих ролей:

- Администратор домена может управлять виртуальными объектами во всех проектах внутри назначенного домена, а также назначением проектов и пользователей на панели самообслуживания.
- Участник проекта играет роль администратора проекта в определенном домене на панели самообслуживания. Участника проектов можно назначить на несколько проектов, тогда он будет управлять виртуальными объектами во всех этих проектах.

С пользователями можно выполнить следующие действия.

- Изменить учетные данные или разрешения пользователя.
- Разрешить или запретить пользователю вход путем включения или отключения учетной записи.
- Удалить пользователя.

С проектами можно выполнить следующие действия.

- Просмотреть квоты проектов.
- Назначить участников на проекты.

Ограничения

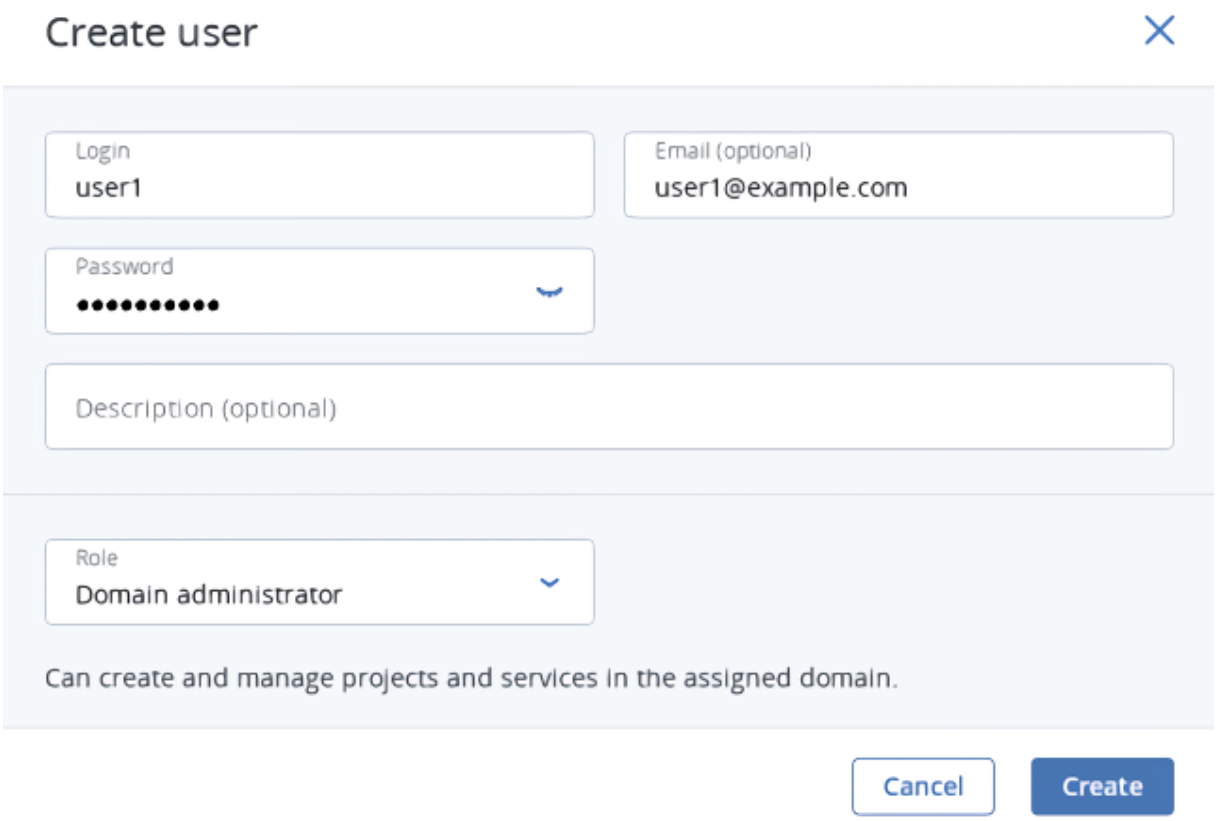
- Только администраторы домена могут управлять пользователями и проектами.

4.1 Создание пользователей

Администраторы домена могут создавать других администраторов домена и участников проекта.

Как создать пользователя

1. Выберите домен из раскрывающегося списка в правом верхнем углу.
2. Откройте экран **Пользователи** и нажмите **Создать пользователя**.
3. В окне **Создать пользователя** укажите имя пользователя, пароль и при необходимости адрес электронной почты и описание. Имя пользователя должно быть уникальным в пределах домена.
4. Выберите нужную роль из раскрывающегося списка **Роль**.
5. Нажмите кнопку **Создать**.

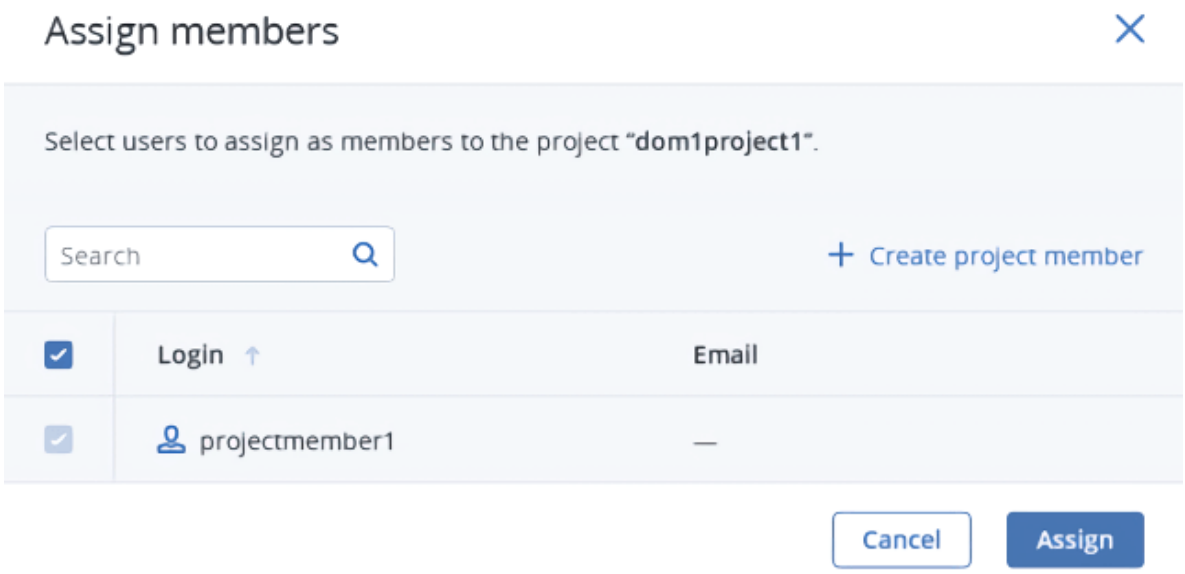


4.2 Назначение пользователей на проекты

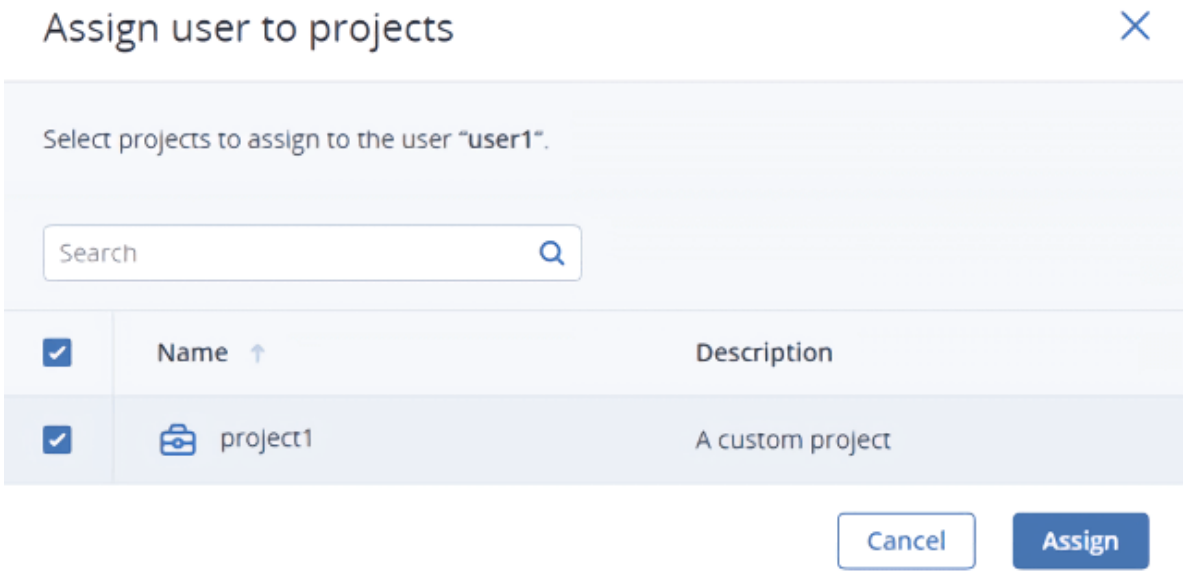
Администраторы домена могут управлять назначением участников проекта на страницах **Проекты** и **Пользователи**.

Как назначить пользователя на проект

- На странице **Проекты**
  1. Нажмите проект, на который нужно назначить пользователей (не имя проекта).
  2. На панели проекта нажмите **Назначить участников**.
  3. В окне **Назначить участников** выберите одного или нескольких пользователей для назначения на проект. Отображаются только учетные записи пользователей с ролью **Участник проекта**. При необходимости нажмите **Создать участника проекта** для создания участника в новом окне.
  4. Нажмите **Назначить**.

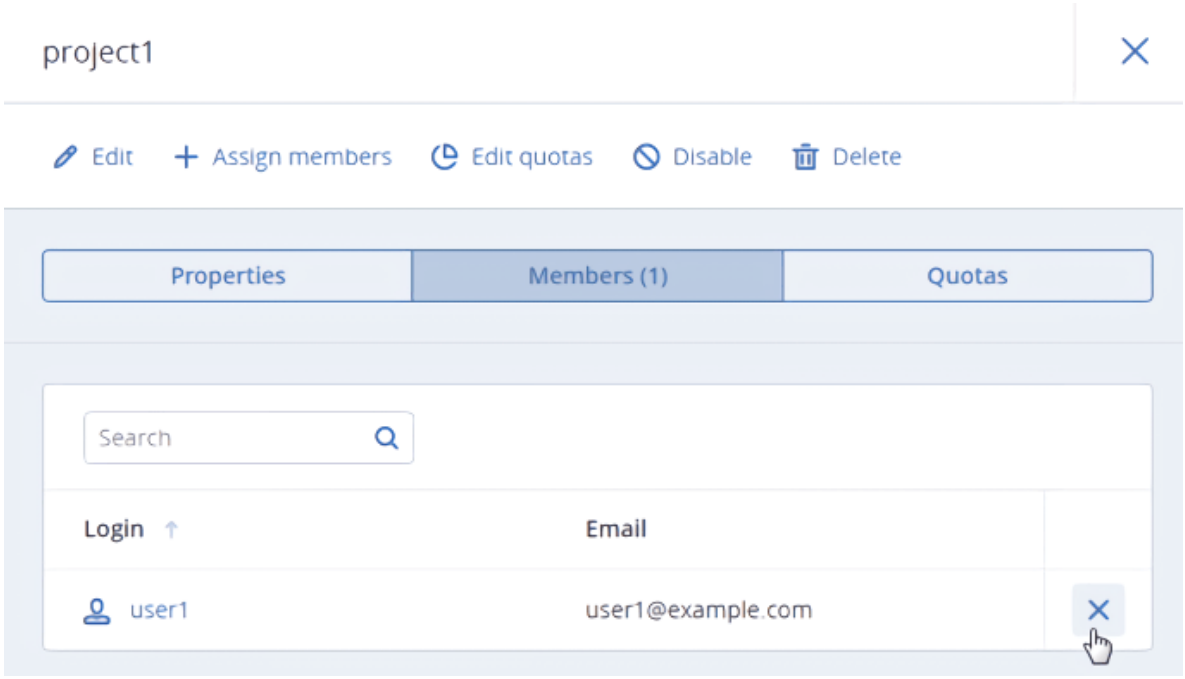


- На странице **Пользователи**
  1. Нажмите учетную запись пользователя с ролью **Участник проекта**, которого необходимо назначить на проект.
  2. На панели пользователя нажмите **Назначить проекту**.
  3. В окне **Назначить пользователя проекту** выберите один или несколько проектов и нажмите **Назначить**.

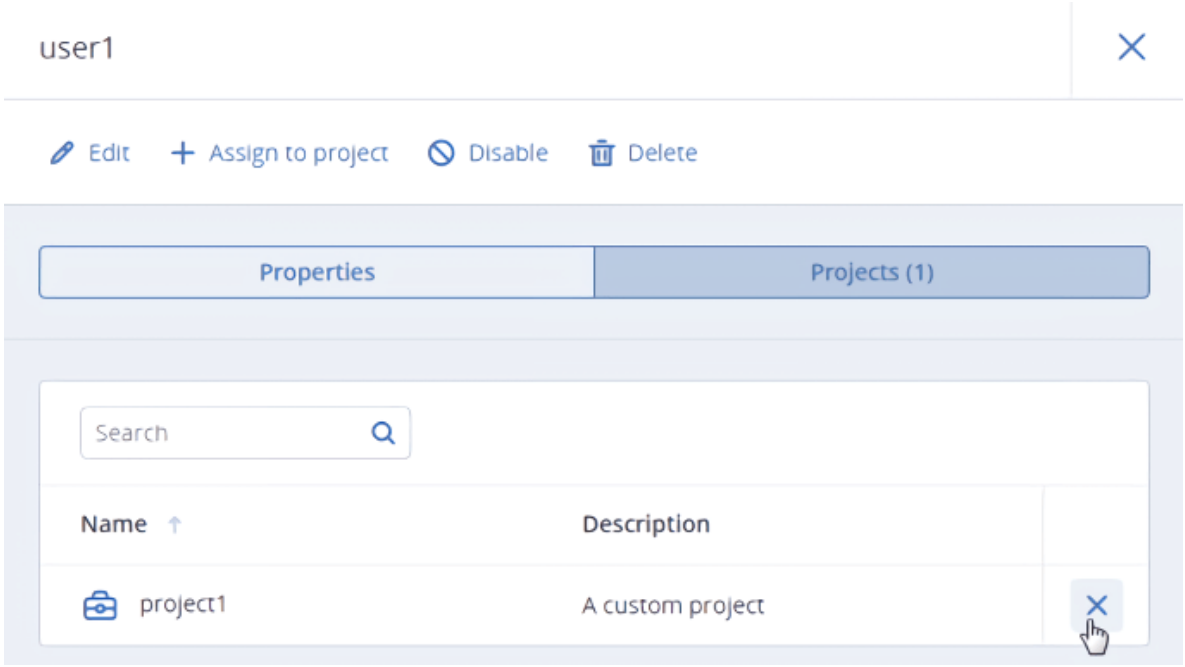


Как снять пользователя с проекта

- На странице **Все проекты**:
  1. Нажмите проект, с которого необходимо снять пользователей.
  2. На панели проекта откройте вкладку **Участники**.
  3. Нажмите крестик рядом с пользователем, которого необходимо снять с проекта.



- На вкладке **Все пользователи**:
  1. Нажмите пользователя, которого необходимо снять с проекта.
  2. На панели пользователя откройте вкладку **Проекты**.
  3. Нажмите крестик рядом с проектом, с которого необходимо снять пользователя.

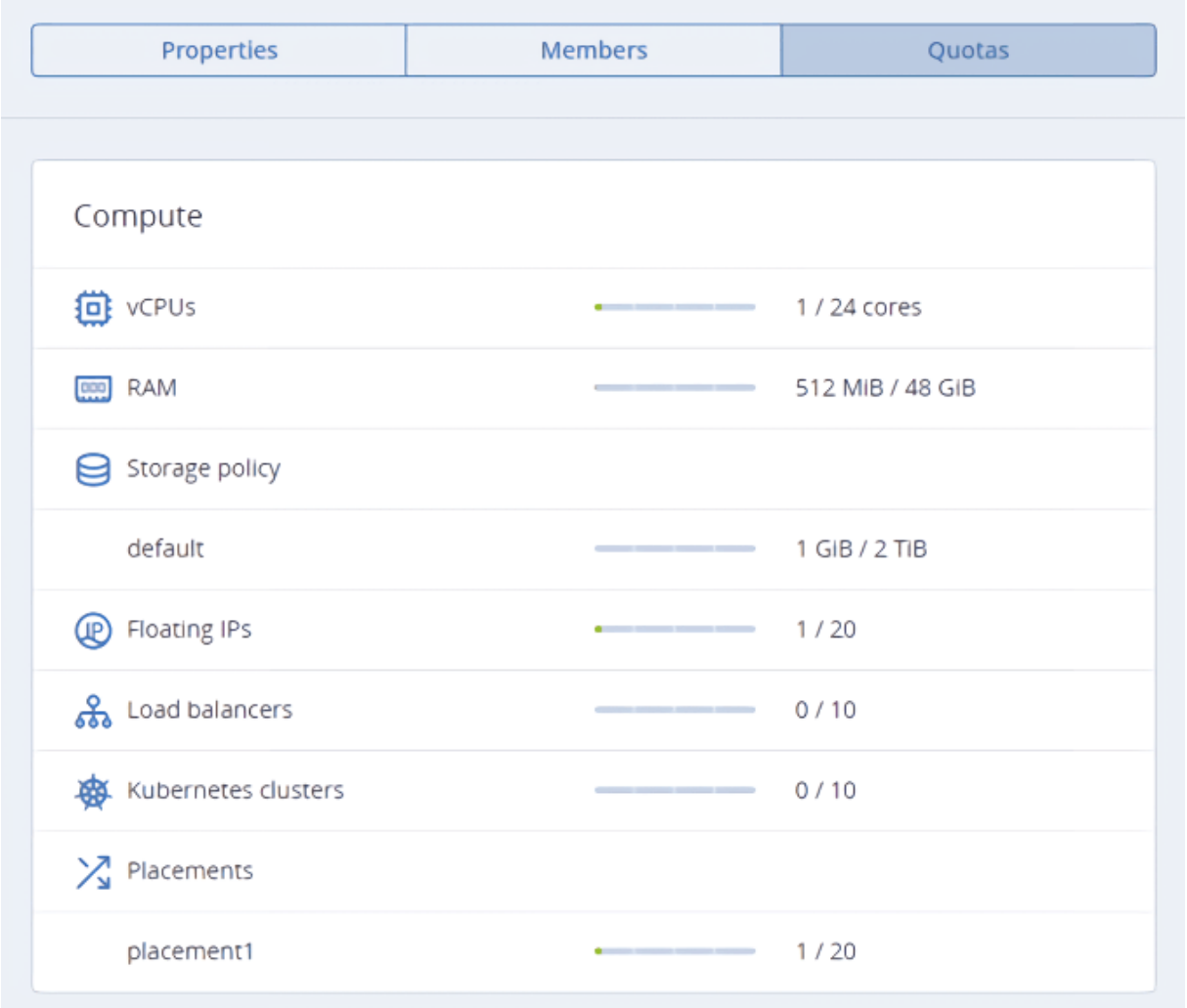


4.3 Просмотр квот проектов

Для каждого проекта выделяется определенный объем вычислительных ресурсов посредством квот. Администраторы домена могут просматривать квоты проекта на экране сведений о проекте.

Как просмотреть квоты проекта

Откройте **Проекты**, нажмите нужный проект в списке и перейдите на вкладку **Квоты**.



5 Управление вычислительными ресурсами

5.1 Управление виртуальными машинами

Каждая виртуальная машина (ВМ) – это независимая система с независимым набором виртуального оборудования. Она имеет следующие основные характеристики.

- Виртуальная машина представляет собой подобие обычного компьютера и работает аналогичным образом. Она имеет собственное виртуальное оборудование. Программные приложения могут работать в виртуальных машинах без каких-либо изменений или специальных настроек.
- Конфигурацию виртуальной машины можно легко изменить, например добавив новые виртуальные диски или память.
- Хотя виртуальные машины совместно используют одни физические аппаратные ресурсы, они полностью изолированы друг от друга (имеют отдельные файловые системы, процессы, переменные sysctl) и от вычислительного сервера.
- На виртуальной машине может работать любая поддерживаемая гостевая операционная система.

В таблице ниже перечислены текущие ограничения для конфигурации виртуальных машин.

Ресурс	Ограничение
ОЗУ	1 ТиБ
ЦП	64 виртуальных ЦП
Хранилище	15 томов по 512 ТиБ каждый
Сеть	15 сетевых адаптеров

5.1.1 Поддерживаемые гостевые операционные системы

Перечисленные ниже гостевые операционные системы прошли тестирование и поддерживаются в виртуальных машинах.

Примечание
Поддерживается только архитектура x64.

Linux

Дистрибутив	Версия	Поддержка горячего подключения ЦП	Поддержка горячего подключения ОЗУ
Alma Linux	9, 8	Да	Да
Astra Linux Common	2.12, 2.11	Да	Да

Дистрибутив	Версия	Поддержка горячего подключения ЦП	Поддержка горячего подключения ОЗУ
Edition			
Astra Linux Special Edition	1.6, 1.5	Да	Да
CentOS	9.x, 8.x, 7.x	Да	Да
	6.x	Нет	Нет
Debian	11.x, 10.x, 9.x	Да	Да
Red Hat Enterprise Linux	9.x, 8.x, 7.x	Да	Да
Rocky Linux	9, 8	Да	Да
Ubuntu	22.04.x, 20,04.x, 18,04.x	Да	Да
	16,04.x	Нет	Нет
Альт Рабочая станция	10, 9	Да	Да
Альт Сервер	10, 9	Да	Да
РЕД ОС	7	Да	Да
РОСА FRESH	R12, R11	Да	Да
РОСА КОБАЛЬТ	7	Да	Да
РОСА ХРОМ	12	Да	Да

Windows

Версия	Выпуск	Поддержка горячего подключения ЦП	Поддержка горячего подключения ОЗУ
Windows Server 2022	Essentials	Нет	Нет
	Standard, Datacenter	Да	Да
Windows Server 2019	Essentials	Нет	Нет
	Standard, Datacenter	Да	Да
Windows Server 2016	Essentials	Нет	Нет
	Standard, Datacenter	Да*	Да
Windows	Essentials, Standard, Datacenter	Да	Да

Версия	Выпуск	Поддержка горячего подключения ЦП	Поддержка горячего подключения ОЗУ
Server 2012 R2			
Windows Server 2012	Standard, Datacenter	Да	Да
Windows Server 2008 R2	Standard, Datacenter	Нет	Нет
Windows 10	Home, Professional, Enterprise, Enterprise 2016 LTSB	Нет	Нет
Windows 8.1	Home, Professional, Enterprise	Нет	Нет
Windows 7	Home, Professional, Enterprise	Нет	Нет

*Горячее подключение ЦП работает некорректно из-за ошибки Windows с неправильно установленным драйвером. Чтобы устранить эту проблему, используйте это решение.

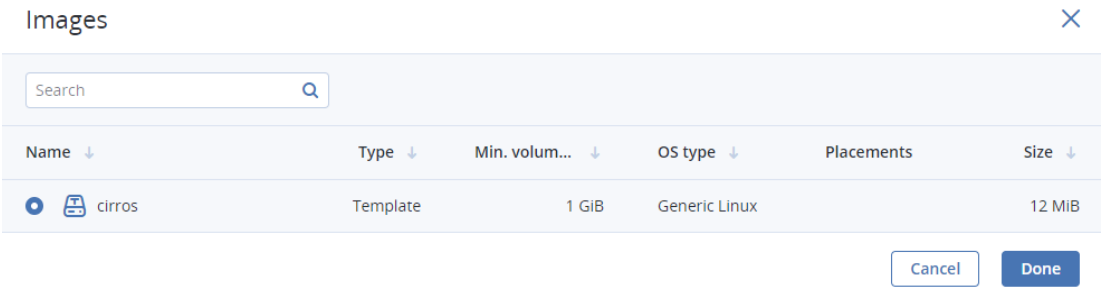
5.1.2 Создание виртуальных машин

Предварительные требования

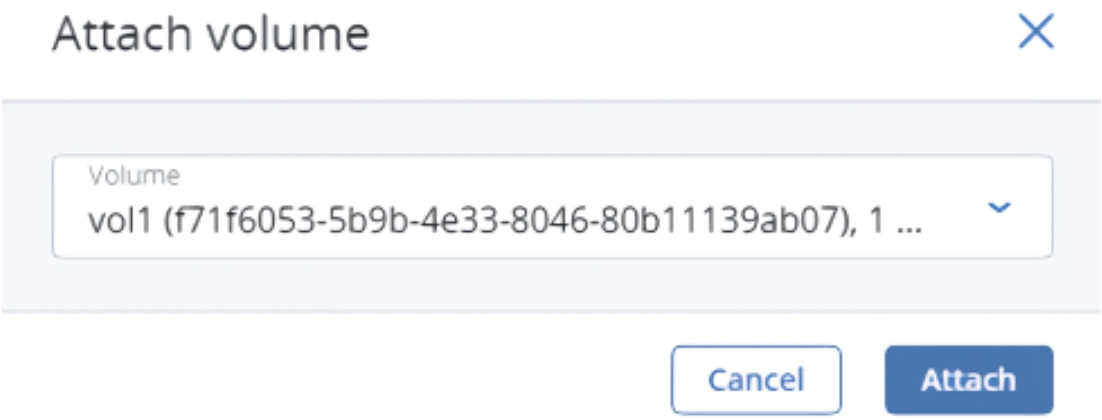
- Подготовлен источник гостевой ОС, как описано в разделе "Управление образами" (стр. 55).
- Созданы одна или несколько вычислительных сетей в соответствии с инструкциями в разделе "Управление виртуальными сетями" (стр. 69).
- [Необязательно] Настроены пользовательские группы безопасности, как указано в разделе "Управление группами безопасности" (стр. 39).
- [Необязательно] Добавлен SSH-ключ, как показано в разделе "Управление SSH-ключами" (стр. 93). SSH-ключ можно указать только при создании ВМ из шаблона или загрузочного тома.

Чтобы создать виртуальную машину

1. На экране **Виртуальные машины** нажмите **Создать виртуальную машину**. Откроется окно, где нужно будет указать параметры ВМ.
2. Укажите имя новой ВМ.
3. Выберите загрузочный носитель ВМ.
   - Если у вас есть ISO-образ или шаблон
     a. Выберите **Образ** в разделе **Развернуть из**, а затем нажмите **Указать** в разделе **Образ**.
     b. В окне **Образы** выберите ISO-образ или шаблон и нажмите **Готово**.



- Если у вас есть вычислительный загрузочный том
  a. Выберите **Том** в разделе **Развернуть из**, а затем нажмите **Указать** в разделе **Тома**.
  b. В окне **Тома** нажмите **Присоединить**.
  c. В окне **Присоединить том** найдите и выберите том и нажмите **Присоединить**.



Если вы присоединяете более одного тома, то первый присоединенный том становится загрузочным по умолчанию. Чтобы выбрать другой том в качестве загрузочного, сделайте его первым в списке, нажимая кнопку со стрелкой вверх.

Примечание
Если выбрать образ или том с назначенным размещением, то созданная ВМ унаследует это размещение.

После выбора загрузочного носителя необходимые для загрузки тома будут автоматически добавлены в раздел **Тома**.

4. Настройте диски ВМ.
   a. В окне **Тома** убедитесь, что загрузочный том по умолчанию достаточно большой для размещения гостевой ОС. В противном случае нажмите значок с многоточием и выберите **Изменить**. Измените размер тома и нажмите **Сохранить**.
   b. [Необязательно] Добавьте дополнительные диски в ВМ путем создания или присоединения томов. Для этого щелкните по значку карандаша в разделе **Тома**, а затем нажмите **Добавить** или **Присоединить** в окне **Тома**.

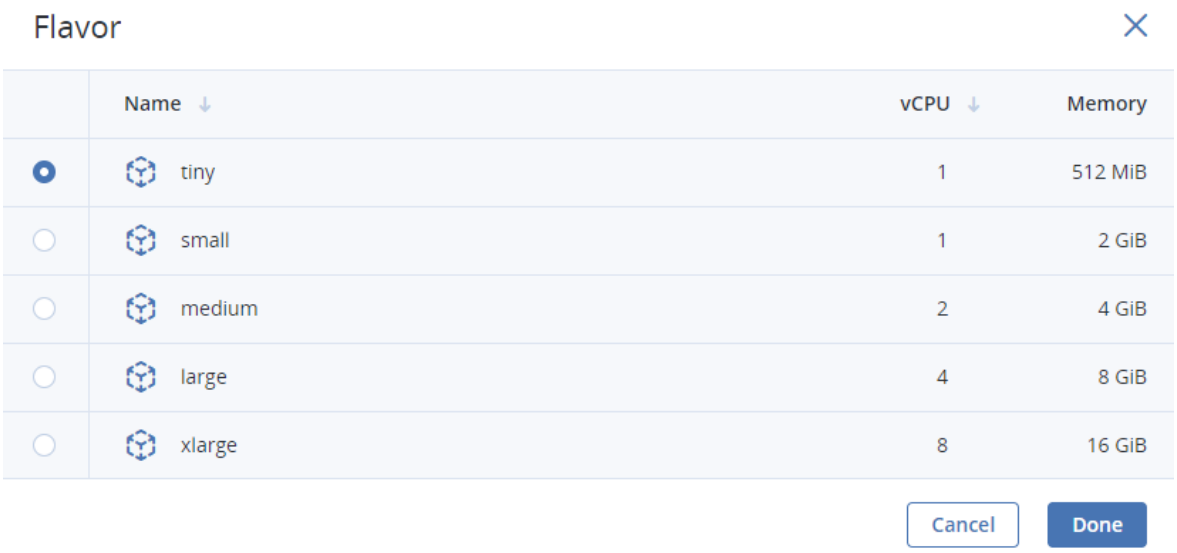
c. Выберите тома, которые будут удалены при удалении ВМ. Для этого щелкните по значку карандаша в разделе **Тома**, нажмите значок с многоточием напротив нужного тома и выберите **Изменить**. Включите параметр **Удалить по завершении** и нажмите **Сохранить**.

d. Завершив настройку дисков ВМ, нажмите **Готово**.

5. Выберите объем ОЗУ и ресурсов ЦП, которые будут выделены ВМ, в разделе **Тип ВМ**. В окне **Тип ВМ** выберите тип и нажмите **Готово**.

Внимание
При выборе типа для ВМ убедитесь, что он удовлетворяет требованиям к оборудованию гостевой ОС.

Примечание
Если выбрать тип ВМ с назначенным размещением, то созданная ВМ унаследует это размещение.



6. Добавьте сетевые интерфейсы для ВМ в разделе **Сети**.

a. В окне **Сетевые интерфейсы** нажмите **Добавить**, чтобы присоединить сетевой интерфейс.

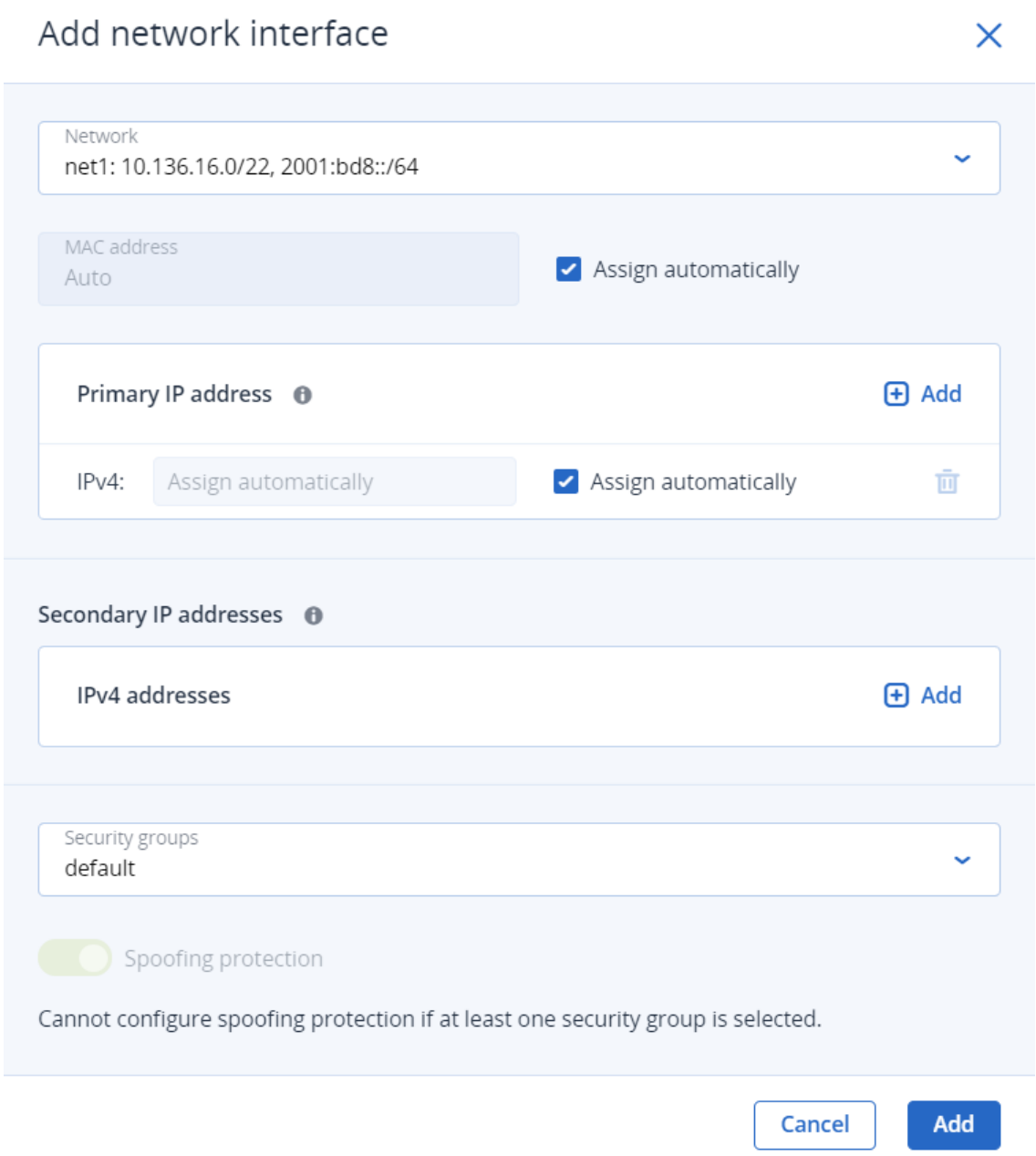
b. В окне **Добавить сетевой интерфейс** выберите вычислительную сеть, к которой следует подключиться, и укажите MAC-адрес, адреса IPv4 и/или IPv6 и группы безопасности. По умолчанию MAC-адрес и основной IP-адрес назначаются автоматически. Чтобы указать их вручную, снимите флажки **Назначить автоматически** и введите нужные адреса. При необходимости можно назначить сетевому интерфейсу дополнительные IP-адреса в разделе **Вторичные IP-адреса**. Учтите, что вторичный адрес IPv6 недоступен для подсети IPv6, которая работает в режиме SLAAC или DHCPv6 без отслеживания состояния.

Примечание

Вторичные IP-адреса, в отличие от основного, не будут автоматически назначены сетевому интерфейсу внутри гостевой ОС виртуальной машины. Их следует назначать вручную.

- Если выбрана виртуальная сеть со включенным управлением IP-адресами
  В этом случае по умолчанию будет включена защита от спуфинга и выбрана группа безопасности **default**. Эта группа безопасности разрешает весь входящий и исходящий трафик на всех портах ВМ. При необходимости можно выбрать другую группу безопасности или несколько групп.

  Чтобы отключить защиту от спуфинга, снимите все флажки и установите переключатель в положение «выкл». С отключенной защитой от спуфинга нельзя настроить группы безопасности.
- Если выбрана виртуальная сеть с отключенным управлением IP-адресами
  В этом случае защита от спуфинга отключена по умолчанию и ее нельзя включить. Для такой сети нельзя настроить группы безопасности.
- Если выбрана общая физическая сеть
  В этом случае пользователь не может самостоятельно настроить защиту от спуфинга. Чтобы включить или отключить защиту от спуфинга, обратитесь к системному администратору.



Указав параметры сетевого интерфейса, нажмите **Добавить**. Интерфейс появится в списке **Сетевые интерфейсы**.

c. [Необязательно] При необходимости измените IP-адреса и группы безопасности добавленных сетевых интерфейсов. Для этого щелкните по значку с многоточием, выберите **Изменить** и задайте нужные параметры.

d. Завершив настройку сетевых интерфейсов ВМ, нажмите **Готово**.

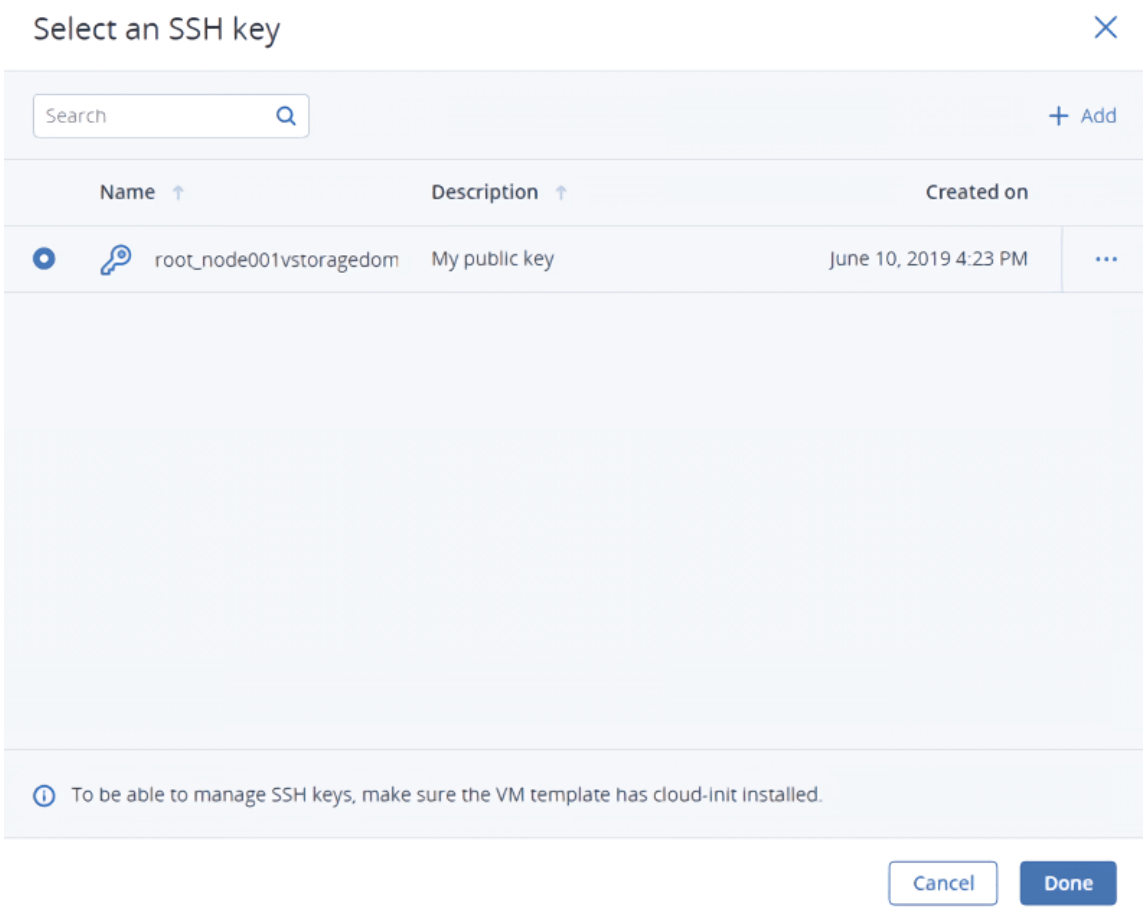
Примечание

Включите EUI-64 в сетевых настройках ВМ для корректного назначения IP-адреса.

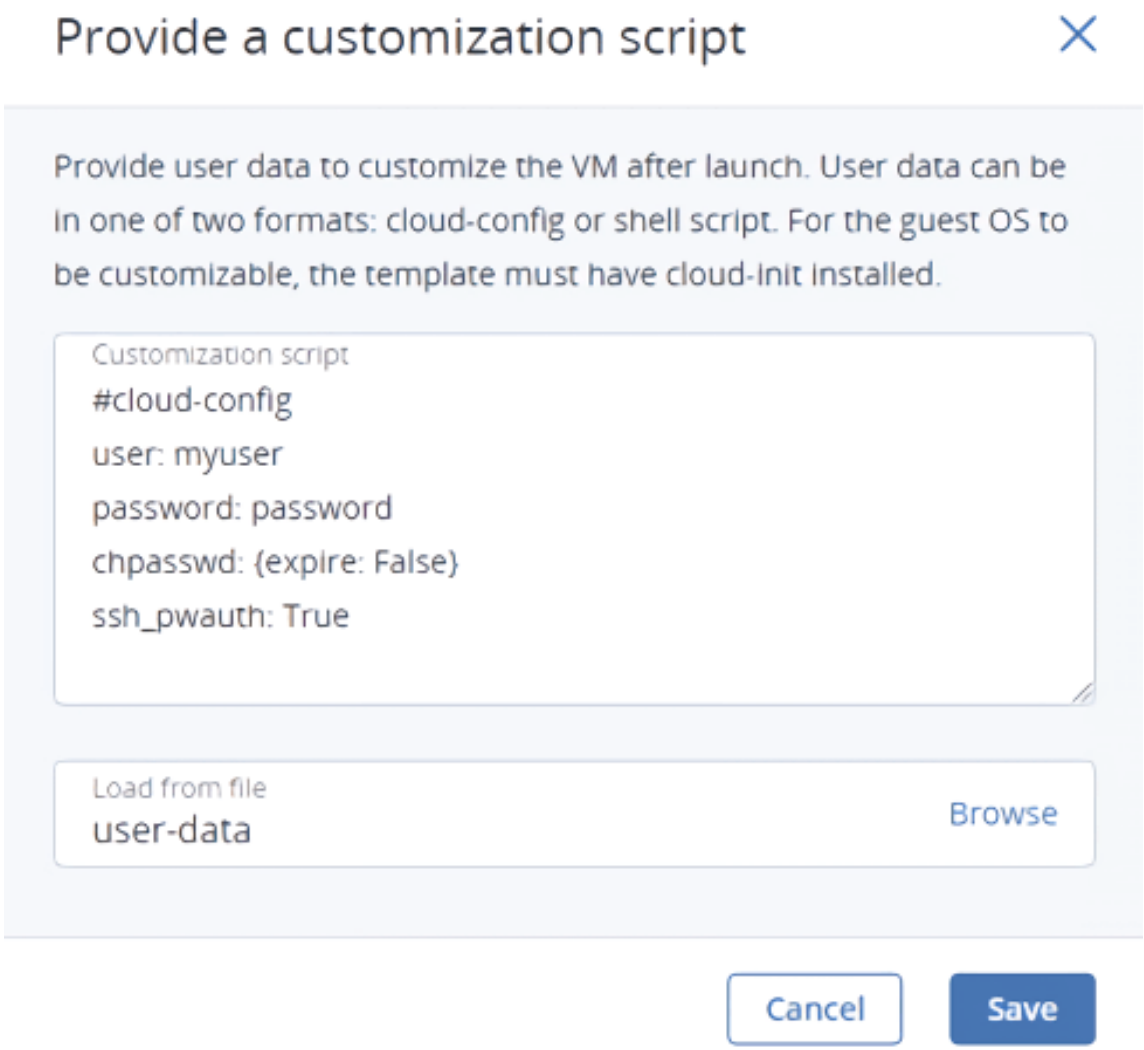
7. [Необязательно] Если вы выбрали загрузку из шаблона или тома, на котором установлены cloud-init и OpenSSH:

Внимание
Поскольку у облачных образов нет пароля по умолчанию, доступ к ВМ, развернутым из этих образов, можно получить только с помощью метода аутентификации с ключом SSH.

- Добавьте SSH-ключ в ВМ, чтобы она была доступна через SSH без пароля.
  В окне **Выберите SSH-ключ** выберите ключ и нажмите **Готово**.



- Добавьте пользовательские данные для настройки ВМ после запуска, например, для изменения пароля пользователя.
  Введите скрипт cloud-config или скрипт оболочки в поле **Скрипт настройки** или укажите файл на локальном сервере, из которого следует загрузить скрипт.



Чтобы внедрить скрипт в виртуальную машину Windows, см. документацию по Cloudbase-Init. Например, можно задать новый пароль для учетной записи с помощью следующего скрипта:

```
#ps1
net user <username> <new_password>
```

8. [Необязательно] В разделе **Расширенные параметры** выполните следующее:
   - Разрешите горячее подключение ресурсов ЦП и ОЗУ для ВМ, чтобы можно было изменить тип работающей ВМ. Горячее подключение также можно разрешить после создания ВМ.

     Примечание
     Если этот параметр не отображается, значит, горячее подключение ресурсов ЦП и ОЗУ в вашем проекте запрещено. Чтобы разрешить его, обратитесь к системному администратору.

   - Запретите автоматические перемещения ВМ, связанные с работой DRS, сняв

установленный по умолчанию флажок **Разрешить автоматические миграции для этой виртуальной машины**. Снять флажок также можно после создания ВМ.

9. Настроив все параметры ВМ, нажмите **Развернуть**, чтобы создать и загрузить ВМ.

Если вы развертываете ВМ из ISO-образа, потребуется установить гостевую ОС внутри ВМ с помощью встроенной консоли VNC. Виртуальные машины, созданные из шаблона или загрузочного тома, уже имеют предустановленную гостевую ОС.

5.1.3 Подключение к виртуальным машинам

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" (стр. 18).
- Чтобы к виртуальной машине можно было подключиться через SSH, в ней должны быть установлены cloud-init и OpenSSH.

Чтобы подключиться к виртуальной машине через консоль VNC

Выберите ВМ и нажмите **Консоль** на ее правой панели. Консоль откроется в новом окне браузера. В консоли можно отправить сочетание клавиш на ВМ, создать снимок экрана окна консоли или скачать файл журнала консоли (см. раздел "Поиск и устранение неисправностей виртуальных машин" (стр. 38)) .

Чтобы подключиться к виртуальной машине через SSH

Укажите имя пользователя и IP-адрес ВМ в терминале SSH.

```
# ssh <username>@<VM_IP_address>
```

Облачные образы Linux имеют имя входа по умолчанию в зависимости от операционной системы, например centos или ubuntu. Чтобы подключиться к ВМ Windows, введите имя пользователя, указанное вами при установке Cloudbase-Init.

Если развертывание ВМ выполнено без указания SSH-ключа, необходимо также ввести пароль для входа в ВМ.

5.1.4 Управление состоянием активности виртуальных машин

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" (стр. 18).

Как управлять состоянием активности виртуальной машины

Щелкните по виртуальной машине или значку многоточия рядом с ней, чтобы открыть полный список действий, доступных для текущего состояния.

- Для запуска ВМ нажмите **Запустить**.
- Для штатной остановки работающей ВМ нажмите **Выключить**. По умолчанию время ожидания остановки, после которого виртуальная машина будет выключена, составляет 10 минут.
- Для принудительной остановки ВМ нажмите **Принудительно выключить**.
- Для мягкой перезагрузки работающей ВМ нажмите **Перезагрузить**.
- Для перезагрузки ВМ без штатной остановки гостевой ОС нажмите **Аппаратная перезагрузка**.
- Для сохранения текущего состояния ВМ в файл нажмите **Приостановить**. Это может пригодиться, например, если необходимо перезапустить хост без выхода из приложений, работающих на ВМ, и без перезапуска ее гостевой ОС.
- Для возвращения ВМ из состояния приостановки нажмите **Возобновить работу**.

5.1.5 Присоединение ISO-образов к виртуальным машинам

Можно присоединить ISO-образы к запущенным или остановленным виртуальным машинам, например, для установки на них дополнительного ПО или восстановления их операционной системы в аварийном режиме. Чтобы присоединить ISO-образ, необходимо преобразовать его в том, а затем присоединить этот том к ВМ.

После завершения установки с ISO-тома его можно отсоединить без предварительной остановки ВМ.

Как создать том из ISO-образа

1. На экране **Образы** щелкните по нужному ISO-образу.
2. На правой панели образа нажмите **Создать том**.
3. В окне **Создать том из образа** укажите имя для тома и нажмите **Создать**.

Как присоединить ISO-том к виртуальной машине

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Тома**.
3. В окне **Тома** нажмите **Присоединить**.
4. В окне **Присоединить том** выберите созданный том и нажмите **Присоединить**. Присоединенный том будет помечен как ISO.
5. В окне **Тома** нажмите **Готово**, чтобы сохранить изменения.

Присоединенный том появится внутри операционной системы ВМ.

Как отсоединить ISO-том от виртуальной машины

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Тома**.
3. В окне **Тома** нажмите значок с многоточием напротив ISO-тома и выберите **Отсоединить**

принудительно.

4. Нажмите **Готово**, чтобы сохранить изменения.

5.1.6 Изменение конфигурации виртуальных машин

После создания виртуальной машины можно управлять ее ресурсами ЦП и ОЗУ, а также сетевыми интерфейсами и томами.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" (стр. 18).

5.1.6.1 Изменение ресурсов виртуальных машин

Можно изменить объем ресурсов ЦП и ОЗУ, используемых виртуальной машиной, применив к ней другой тип ВМ. Для изменения размера работающей ВМ необходимо сначала разрешить для нее горячее подключение ЦП и ОЗУ. Настройки горячего подключения можно изменить как для новых, так и для существующих ВМ.

Запущенная виртуальная машина имеет лимит изменения размера, определяющий максимальное число виртуальных ЦП и максимальный объем ОЗУ, которые можно выделить этой ВМ. Лимит изменения размера для виртуальных ЦП является статическим и равен 64 для всех ВМ. Лимит изменения размера для ОЗУ, напротив, является динамическим и зависит от объема ОЗУ, который запущенная ВМ использует в настоящее время. Этот лимит обновляется при запуске ВМ, а его значения перечислены в таблице ниже.

Текущий размер ОЗУ в ГиБ	Ограничение размера ОЗУ в ГиБ
1-4	16
5-8	32
9-16	64
17-32	128
33-64	256
65-128	512
129-256	1024

Например, можно изменить размер запущенной ВМ, изменив тип ВМ с 16 ГиБ ОЗУ на тип ВМ с 256 ГиБ в два подхода.

1. Измените размер ВМ, установив тип ВМ с 64 ГиБ.
2. Выключите ВМ и запустите ее снова, чтобы обновить лимит изменения размера.
3. Измените размер ВМ, установив тип ВМ с 256 ГиБ.

Ограничения

- Нельзя изменить тип для ВМ с освобожденными ресурсами. Чтобы изменить размер такой ВМ, сначала назначьте ей ресурсы.
- Нельзя уменьшить число ЦП и объем ОЗУ для запущенных ВМ.
- [Для всех гостевых систем Linux] Если в ВМ не установлены дополнения гостевой ОС, новые ядра могут быть в состоянии офлайн после горячего подключения ЦП. Проверить, какие ядра ЦП находятся в состоянии онлайн, можно с помощью команды cat /sys/devices/system/cpu/online. Чтобы активировать ядра ЦП в состоянии офлайн, выполните команду echo 1 > /sys/devices/system/cpu/cpu<cpu_number>/online.

Предварительные требования

- Перед изменением типа ВМ убедитесь, что сервер, на котором размещена ВМ, имеет достаточно ресурсов ЦП и ОЗУ для нового размера ВМ.
- Горячее подключение ЦП и ОЗУ должно быть разрешено системным администратором.
- Перед изменением размера запущенной ВМ убедитесь, что гостевая операционная система поддерживает горячее подключение ЦП и ОЗУ (см. раздел "Поддерживаемые гостевые операционные системы" (стр. 16)). Учтите, что в противном случае после изменения размера гостевая ОС может работать нестабильно. Чтобы увеличить ресурсы ЦП и ОЗУ для такой гостевой ОС, необходимо сначала остановить виртуальную машину.
- Перед изменением размера запущенной ВМ убедитесь, что в гостевой операционной системе установлены последние обновления.

Как разрешить или запретить горячее подключение ЦП и ОЗУ для виртуальной машины

1. На экране **Виртуальные машины** убедитесь, что нужная виртуальная машина находится в состоянии «Выключена», и щелкните по ней.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Горячее подключение ЦП и ОЗУ**.

   Примечание
   Если это поле не отображается, значит, горячее подключение ресурсов ЦП и ОЗУ в вашем проекте запрещено. Чтобы разрешить его, обратитесь к системному администратору.

3. Установите или снимите флажок **Разрешить горячее подключение**, а затем нажмите галочку, чтобы сохранить изменения.

Если горячее подключение ЦП и ОЗУ разрешено, можно изменять тип для работающей ВМ.

Как изменить тип виртуальной машины

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** щелкните по значку карандаша в поле **Тип ВМ**.
3. В окне **Тип ВМ** выберите новый тип ВМ и нажмите **Готово**.

5.1.6.2 Настройка сетевых интерфейсов виртуальных машин

Можно добавить новые сетевые интерфейсы к виртуальным машинам, изменить IP-адреса и группы безопасности для существующих интерфейсов, а также удалить сетевые интерфейсы, отсоединив их.

Ограничения

- Нельзя управлять сетевыми интерфейсами ВМ с освобожденными ресурсами.
- ВМ, подключенная к сети с двойным стеком, всегда получает адрес IPv6, если подсеть IPv6 работает в режиме SLAAC или DHCPv6 без отслеживания состояния.

Чтобы присоединить сетевой интерфейс к виртуальной машине

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите **Изменить** в разделе **Сетевые интерфейсы**.
3. В окне **Сетевые интерфейсы** нажмите **Добавить**, чтобы присоединить сетевой интерфейс.
4. В окне **Добавить сетевой интерфейс** выберите вычислительную сеть, к которой следует подключиться, и укажите MAC-адрес, адреса IPv4 и/или IPv6 и группы безопасности. По умолчанию MAC-адрес и основной IP-адрес назначаются автоматически. Чтобы указать их вручную, снимите флажки **Назначить автоматически** и введите нужные адреса. При необходимости можно назначить сетевому интерфейсу дополнительные IP-адреса в разделе **Вторичные IP-адреса**. Учтите, что вторичный адрес IPv6 недоступен для подсети IPv6, которая работает в режиме SLAAC или DHCPv6 без отслеживания состояния.

   Примечание
   Вторичные IP-адреса, в отличие от основного, не будут автоматически назначены сетевому интерфейсу внутри гостевой ОС виртуальной машины. Их следует назначать вручную.

   - Если выбрана виртуальная сеть со включенным управлением IP-адресами
     В этом случае по умолчанию будет включена защита от спуфинга и выбрана группа безопасности **default**. Эта группа безопасности разрешает весь входящий и исходящий трафик на всех портах ВМ. При необходимости можно выбрать другую группу безопасности или несколько групп.

     Чтобы отключить защиту от спуфинга, снимите все флажки и установите переключатель в положение «выкл». С отключенной защитой от спуфинга нельзя настроить группы безопасности.
   - Если выбрана виртуальная сеть с отключенным управлением IP-адресами
     В этом случае защита от спуфинга отключена по умолчанию и ее нельзя включить. Для такой сети нельзя настроить группы безопасности.
   - Если выбрана общая физическая сеть
     В этом случае пользователь не может самостоятельно настроить защиту от спуфинга. Чтобы включить или отключить защиту от спуфинга, обратитесь к системному администратору.

Указав параметры сетевого интерфейса, нажмите **Добавить**.

5. Нажмите **Готово**, чтобы завершить настройку сетевых интерфейсов ВМ и сохранить изменения.

Чтобы изменить сетевой интерфейс виртуальной машины

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите **Изменить** в разделе **Сетевые интерфейсы**.
3. В окне **Сетевые интерфейсы** нажмите кнопку с многоточием напротив нужного сетевого интерфейса и выберите **Изменить**.
4. В окне **Изменить сетевой интерфейс** измените параметры сетевого интерфейса следующим образом:
   - Измените основной IP-адрес. Чтобы обновить адрес внутри гостевой ОС виртуальной машины, перезапустите сетевой интерфейс.
   - Добавьте или удалите вторичные IP-адреса.
   - Измените группы безопасности, назначенные виртуальной машине.

   Обновив нужные параметры, нажмите **Сохранить**.
5. Нажмите **Готово**, чтобы завершить настройку сетевых интерфейсов ВМ и сохранить изменения.

Чтобы отсоединить сетевой интерфейс от виртуальной машины

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите **Изменить** в разделе **Сетевые интерфейсы**.
3. В окне **Сетевые интерфейсы** нажмите кнопку с многоточием напротив сетевого интерфейса, который следует отсоединить, и выберите **Удалить**.
4. Нажмите **Готово**, чтобы завершить настройку сетевых интерфейсов ВМ и сохранить изменения.

5.1.6.3 Настройка томов виртуальных машин

Можно добавлять новые тома к виртуальным машинам, присоединять существующие тома и отсоединять ненужные.

Ограничения

- Нельзя изменить, отсоединить или удалить загрузочный том.
- Присоединять и отсоединять можно только незагрузочные тома.
- Нельзя управлять томами ВМ с освобожденными ресурсами.

Предварительные требования

- Чтобы можно было использовать тома, присоединенные к ВМ, они должны быть инициализированы внутри гостевой ОС стандартными средствами.

Как присоединить том к виртуальной машине

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Тома**.
3. В окне **Тома**:
   - Нажмите **Присоединить** для присоединения существующего тома, а затем выберите том в окне **Присоединить том**.
   - Нажмите **Добавить**, чтобы создать новый том, а затем укажите для него имя, размер и политику хранилища. Созданный том будет автоматически добавлен к дискам ВМ.
4. Нажмите **Готово**, чтобы завершить настройку дисков ВМ и сохранить изменения.

Как отсоединить том от виртуальной машины

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** нажмите значок карандаша в поле **Тома**.
3. В окне **Тома**:
   - Нажмите **Отсоединить**, чтобы отсоединить том от остановленной виртуальной машины.
   - Нажмите **Отсоединить принудительно**, чтобы отсоединить том от работающей виртуальной машины.

     Предупреждение
     При этом есть риск потери данных.
4. Нажмите **Готово**, чтобы завершить настройку дисков ВМ и сохранить изменения.

5.1.7 Мониторинг виртуальных машин

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" (стр. 18).

Как отслеживать потребление виртуальной машиной ресурсов ЦП, хранилища и сети

Выберите ВМ и откройте вкладку **Мониторинг**.

Интервал времени для диаграмм по умолчанию составляет двенадцать часов. Чтобы рассмотреть определенный интервал времени в большем масштабе, выделите его мышью; чтобы восстановить прежний масштаб, дважды щелкните по любой диаграмме.

Доступны следующие диаграммы производительности:

ЦП/ОЗУ
Использование ЦП и ОЗУ виртуальной машиной.

Сеть
Входящий и исходящий сетевой трафик.

Чтение/запись в хранилище
Объем данных, считанных и записанных виртуальной машиной.

Задержка чтения/записи

Задержка чтения и записи. Наведя указатель мыши на ту или иную точку диаграммы, можно также просмотреть среднюю и максимальную задержку на соответствующий момент, а также 95-й и 99-й процентили.

Примечание
Средние значения рассчитываются каждые пять минут.

5.1.8 Освобождение ресурсов виртуальных машин

Можно отменить привязку остановленной ВМ к серверу, где она была размещена, и высвободить ее зарезервированные ресурсы, такие как ЦП и ОЗУ. При этом ВМ остается загружаемой и сохраняет свою конфигурацию, включая IP-адреса.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" (стр. 18).

Как освободить ресурсы остановленной виртуальной машины

1. Щелкните по остановленной виртуальной машине.
2. На правой панели ВМ нажмите **Освободить ресурсы**.

Как освободить ресурсы работающей или приостановленной виртуальной машины

1. Щелкните по работающей или приостановленной виртуальной машине.
2. На правой панели ВМ нажмите **Выключить** или **Принудительно выключить**, а затем выберите **Освободить ресурсы ВМ** в окне подтверждения.

Как воссоздать освобожденную ВМ на сервере с достаточным для нее количеством ресурсов

1. Щелкните по виртуальной машине с освобожденными ресурсами.
2. На правой панели ВМ нажмите **Назначить ресурсы**.

5.1.9 Аварийное восстановление виртуальных машин

Если возникают проблемы с загрузкой ВМ, можно перевести ее в режим аварийного восстановления для доступа к загрузочному тому. Когда ВМ в состоянии «Запущена» переводится в режим аварийного восстановления, сначала выполняется мягкая остановка. После того как ВМ перейдет в режим аварийного восстановления, к ней можно подключиться через SSH или консоль. Предыдущий загрузочный диск ВМ теперь присоединен как вторичный. Можно подключить этот диск и исправить на нем ошибки.

Ограничения

- В режиме аварийного восстановления ISO-образы могут использоваться для загрузки виртуальных машин как Linux, так и Windows, а образы (шаблоны) QCOW2 – для загрузки ВМ Linux. Для инструкций о создании шаблонов см. раздел "Подготовка шаблонов" (стр. 57).

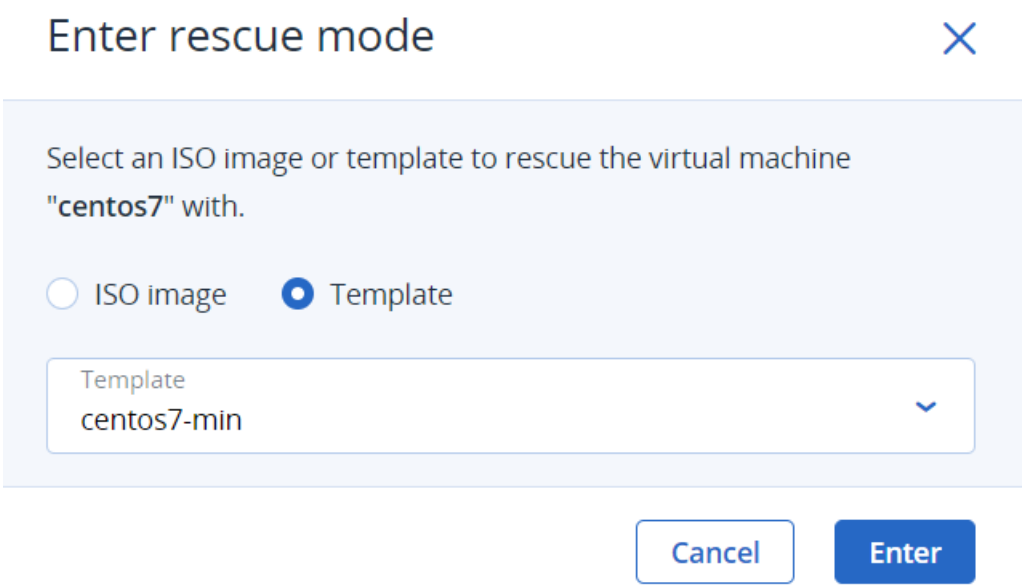
- ВМ можно перевести в режим аварийного восстановления, только если ее текущее состояние «Запущена» или «Выключена».
- Для ВМ в режиме аварийного восстановления доступны только три действия: **Консоль**, **Выйти из режима восстановления** и **Удалить**.
- Если в образе для аварийного восстановления установлен пакет cloud-init, то к ВМ, загруженной из образа, можно будет получить доступ с помощью того же SSH-ключа, который использовался для ее создания.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" (стр. 18).

Как перевести виртуальную машину в режим аварийного восстановления

1. На экране **Виртуальные машины** щелкните по нужной ВМ в списке.
2. На правой панели ВМ нажмите кнопку с многоточием на панели инструментов. Затем нажмите **Войти в режим восстановления**.
3. В окне **Войти в режим восстановления** выберите образ для восстановления ВМ. По умолчанию выбран образ, который использовался для создания ВМ. Нажмите **Войти**.



Статус машины изменится на «Восстановление».

Как вернуть виртуальную машину в режим нормальной работы

1. На экране **Виртуальные машины** щелкните по нужной ВМ в списке.
2. На правой панели ВМ нажмите **Выйти из режима восстановления**.
3. В окне **Выйти из режима восстановления** нажмите **Выйти**. ВМ автоматически перезагрузится.

Статус ВМ сменится на «Запущена», и ВМ загрузится с исходного корневого диска.

Примечание

Если при выходе из режима аварийного восстановления статус ВМ изменится на «Ошибка», его можно сбросить с помощью действия **Сбросить состояние**. После этого ВМ должна вернуться в состояние «Восстановление».

Выход из режима аварийного восстановления для виртуальных машин Windows

При выходе ВМ Windows из режима аварийного восстановления может возникать проблема. Если в этом режиме установить статус «в сети» для исходного системного диска, то его идентификатор становится таким же, как идентификатор диска аварийного восстановления. После этого при попытке выйти из режима аварийного восстановления загрузчик не может найти правильный загрузочный диск. Чтобы разрешить конфликт идентификаторов, выполните следующие действия.

1. Когда ВМ находится в режиме аварийного восстановления, откройте окно **Управление дисками** и запомните номер исходного системного диска (не в сети) и диска аварийного восстановления (в сети). Установите для исходного системного диска статус **В сети**.
2. Чтобы изменить конфигурацию загрузки, введите следующую команду в окне **Командная строка**:

   ```
   > bcdedit /store <the original system disk name>:\boot\bcd
   ```

3. Просмотрите выходные данные и убедитесь, что диск аварийного восстановления является целевым для объектов (partition=<the rescue disk name>).

   Если объекты не указывают на диск C, исправьте это следующими командами:

   ```
   > bcdedit /store <the original system disk name>:\boot\bcd \
   /set {default} osdevice partition=<the rescue disk name>:
   > bcdedit /store <the original system disk name>:\boot\bcd \
   /set {default} device partition=<the rescue disk name>:
   > bcdedit /store <the original system disk name>:\boot\bcd \
   /set {bootmgr} device partition=<the rescue disk name>:
   > bcdedit /store <the original system disk name>:\boot\bcd \
   /set {memdiag} device partition=<the rescue disk name>:
   ```

4. Чтобы просмотреть доступные диски, введите в командной строке следующие команды:

   ```
   > DISKPART
   > LIST DISK
   ```

   Сопоставьте номер и имя диска с указанными в окне **Управление дисками**.

5. Чтобы получить идентификатор диска аварийного восстановления, выполните следующие команды:

   ```
   > SELECT DISK <the rescue disk number>
   > UNIQUEID DISK
   ```

   Запишите идентификатор диска, он понадобится позже.

6. Измените этот идентификатор с помощью следующей команды:

   ```
   > UNIQUEID DISK id=<any hex value of 8 characters>
   ```

   Убедитесь, что значение изменилось, с помощью команды UNIQUEID DISK.
7. Назначьте исходному системному диску записанный ранее идентификатор.

   ```
   > SELECT DISK <the original system disk number>
   > UNIQUEID DISK id=<the recorded disk ID>
   ```

   Убедитесь, что значение изменилось, с помощью команды UNIQUEID DISK.

Теперь можно будет выйти из режима аварийного восстановления.

Как добавить драйверы дисков в среду восстановления Windows (Windows Recovery Environment)

Для отображения дисков виртуальной машины в среде восстановления Windows необходимо, чтобы в WIM-образе, используемом для загрузки среды восстановления, присутствовали необходимые драйверы. Эти драйверы расположены на диске A:, который подключен по умолчанию к виртуальным машинам с операционной системой Windows.

Например, чтобы добавить необходимые драйверы в WIM-образ среды восстановления Windows на рабочей виртуальной машине, выполните следующие действия:

1. Запустите интерпретатор командной строки от имени администратора.
2. Создайте папку, к которой будет подключен WIM-образ среды восстановления. Например:

   ```
   md C:\mount
   ```
3. Подключите WIM-образ среды восстановления к созданной папке. Например:

   ```
   ReAgentC.exe /mountre /path c:\mount
   ```
4. Добавьте необходимые драйверы в подключенный WIM-образ. Например:

   ```
   Dism /Image:C:\mount /Add-Driver /Driver:"A:\Drivers\NetKVM\w10\amd64\netkvm.inf"
   Dism /Image:C:\mount /Add-Driver /Driver:"A:\Drivers\vioscsi\w10\amd64\vioscsi.inf"
   Dism /Image:C:\mount /Add-Driver /Driver:"A:\Drivers\viostor\w10\amd64\viostor.inf"
   ```
5. Сохраните изменения и отключите WIM-образ от папки. Например:

   ```
   ReAgentC.exe /unmountre /path c:\mount /commit
   ```

После загрузки среды восстановления Windows, использующей обновленный WIM-образ, будут отображаться диски виртуальной машины.

5.1.10 Управление дополнениями гостевой ОС

В этом разделе описывается, как установить и удалить дополнения гостевой ОС. Эти функции требуются для создания согласованных моментальных снимков дисков работающей ВМ.

Ограничения

- Дополнения гостевой ОС зависят от гостевого агента QEMU, который устанавливается вместе с ними. Для работы дополнений должна быть запущена служба агента.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" (стр. 18).
- В виртуальной машине установлена гостевая операционная система.

5.1.10.1 Установка дополнений гостевой ОС

Примечание
Виртуальная машина должна иметь доступ к Интернету.

1. Создайте вычислительный том из образа **vz-guest-tools-win** или **vz-guest-tools-lin** в зависимости от операционной системы ВМ.

   Примечание
   Если в вашем проекте нет этих образов, обратитесь к системному администратору.

   a. На экране **Образы** щелкните по образу **vz-guest-tools-win** или **vz-guest-tools-lin**.
   b. На правой панели образа нажмите **Создать том**.
   c. В окне **Создать том из образа** укажите имя для тома и нажмите **Создать**.
2. Присоедините том с дополнениями гостевой ОС к виртуальной машине.
   a. На экране **Виртуальные машины** щелкните по нужной ВМ.
   b. На правой панели ВМ нажмите значок карандаша в поле **Тома**.
   c. В окне **Тома** нажмите **Присоединить**.
   d. В окне **Присоединить том** выберите созданный том с дополнениями гостевой ОС и нажмите **Присоединить**. Присоединенный том будет помечен как ISO.
   e. В окне **Тома** нажмите **Готово**, чтобы сохранить изменения.
3. Выполните вход в виртуальную машину.
4. Внутри ВМ выполните следующие действия.
   - Внутри ВМ Windows перейдите на подключенный оптический диск в проводнике и установите дополнения гостевой ОС, запустив файл setup.exe. После завершения установки перезапустите ВМ.

- Внутри ВМ Linux установите пакет с заголовками или исходными кодами ядра. Версия пакета должна соответствовать версии ядра.

  Затем создайте точку подключения для оптического диска с образом дополнений гостевой ОС и запустите установщик.

  ```
  # mkdir /mnt/cdrom
  # mount <path_to_guest_tools_iso> /mnt/cdrom
  # bash /mnt/cdrom/install
  ```

5.1.10.2 Удаление дополнений гостевой ОС

Если окажется, что дополнения гостевой ОС несовместимы с каким-либо ПО внутри виртуальной машины, их можно удалить следующим образом.

- Внутри ВМ Windows:
  1. Удалите драйверы устройств QEMU из диспетчера устройств.

     Внимание
     Не удаляйте драйвер жесткого диска VirtIO/SCSI и сетевой драйвер NetKVM. Без первого драйвера ВМ не будет загружаться, а без второго потеряет возможность подключения к сети.

  2. Удалите гостевой агент QEMU и дополнения гостевой ОС из списка установленных приложений.
  3. Остановите и удалите **Guest Tools Monitor**.

     ```
     > sc stop VzGuestToolsMonitor
     > sc delete VzGuestToolsMonitor
     ```

  4. Отмените регистрацию **Guest Tools Monitor** в **журнале событий**.

     ```
     > reg delete HKLM\SYSTEM\CurrentControlSet\services\eventlog\Application\\
     VzGuestToolsMonitor
     ```

  5. Удалите раздел реестра для автозапуска **RebootNotifier**.

     ```
     > reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v \
     VzRebootNotifier
     ```

  6. Удалите папку C:\Program Files\Qemu-ga\.

     Если файл VzGuestToolsMonitor.exe заблокирован, закройте все окна средства просмотра событий. Если файл остается заблокированным, перезапустите службу eventlog.

     ```
     > sc stop eventlog
     > sc start eventlog
     ```

  После удаления дополнений гостевой ОС перезапустите виртуальную машину.
- Внутри ВМ Linux:

1. Удалите пакеты.
   - В системах на базе RPM (CentOS и др.):

     ```
     # yum remove dkms-vzvirtio_balloon prl_nettool qemu-guest-agent-vz \
     vz-guest-udev
     ```

   - В системах на базе DEB (Debian и Ubuntu):

     ```
     # apt-get remove vzvirtio-balloon-dkms prl-nettool qemu-guest-agent-vz \
     vz-guest-udev
     ```

     Если какие-либо из перечисленных выше пакетов не установлены в системе, выполнение команды завершится ошибкой. В этом случае исключите эти пакеты из команды и выполните ее снова.
2. Удалите файлы.

   ```
   # rm -f /usr/bin/prl_backup /usr/share/qemu-ga/VERSION \
   /usr/bin/install-tools \
   /etc/udev/rules.d/90-guest_iso.rules /usr/local/bin/fstrim-static \
   /etc/cron.weekly/fstrim
   ```

3. Перезагрузите правила udev.

   ```
   # udevadm control --reload
   ```

После удаления дополнений гостевой ОС перезапустите виртуальную машину.

5.1.11 Поиск и устранение неисправностей виртуальных машин

Если не удается развернуть виртуальную машину

Просмотрите сообщение об ошибке на правой панели ВМ. Одной из возможных причин сбоя может быть нехватка свободных ресурсов ОЗУ или ЦП для размещения ВМ.

Если виртуальная машина зависла в состоянии сбоя или переходном состоянии

Сбросьте ВМ в последнее стабильное состояние: активное, выключенное или с освобожденными ресурсами.

1. Щелкните по зависшей ВМ.
2. На правой панели ВМ нажмите **Сбросить состояние**.

Если не удается загрузить виртуальную машину

Просмотрите журнал консоли ВМ, нажав **Загрузить журнал консоли** на правой панели ВМ. Журнал будет содержать сообщения, только если ведение журнала включено внутри ВМ (см. "Включение ведения журнала для виртуальных машин" (стр. 62)).

5.1.12 Удаление виртуальных машин

Ограничения

- ВМ удаляется вместе с ее дисками, у которых при развертывании ВМ был включен параметр **Удалить по завершении**.

Предварительные требования

- Созданы виртуальные машины, как описано в разделе "Создание виртуальных машин" (стр. 18).

Как удалить одну виртуальную машину

1. Нажмите кнопку с многоточием напротив ВМ, которую следует удалить, и выберите **Удалить**.
2. Нажмите **Удалить** в окне подтверждения.

Как удалить несколько виртуальных машин

1. Установите флажки напротив ВМ, которые следует удалить.
2. Над списком ВМ нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

5.2 Управление группами безопасности

Группа безопасности – это набор правил сетевого доступа, которые контролируют входящий и исходящий трафик виртуальных машин, назначенных в эту группу. С помощью правил группы безопасности можно задать тип и направление трафика, которому разрешен доступ к порту виртуального интерфейса. Трафик, не соответствующий ни одному правилу, отбрасывается.

Для каждого проекта в вычислительном кластере автоматически создается группа безопасности **default** (по умолчанию). Эта группа разрешает весь трафик на всех портах для всех протоколов, и удалить ее нельзя. Когда вы присоединяете сетевой интерфейс к ВМ, он привязывается к группе безопасности **default**, если не выбрана пользовательская группа безопасности.

Как новым, так и существующим виртуальным машинам можно назначить одну или несколько групп безопасности. При добавлении или удалении правил из групп безопасности эти изменения принудительно применяются во время выполнения.

Ограничения

- Можно управлять только правилами групп безопасности IPv4.

5.2.1 Создание и удаление групп безопасности

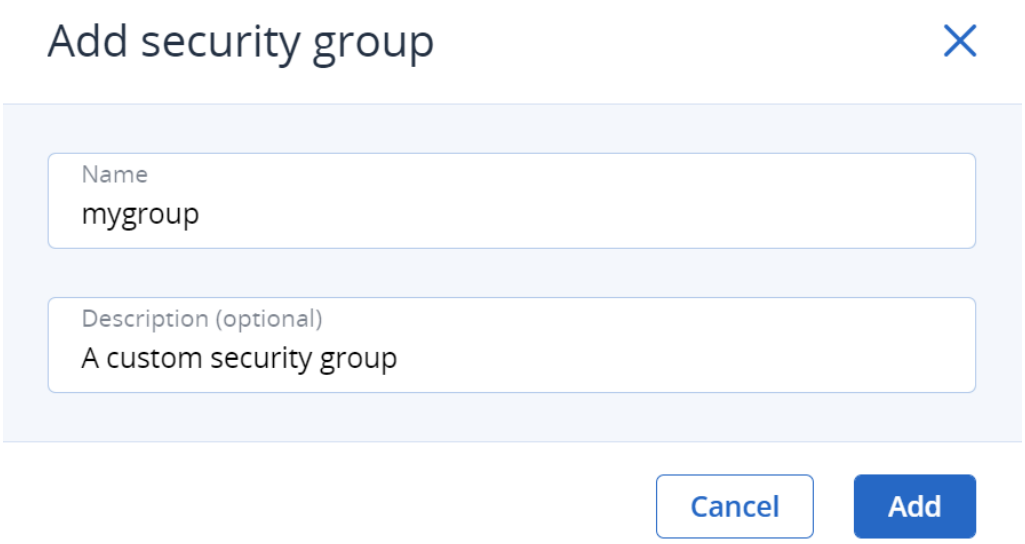
Ограничения

- Группу безопасности нельзя удалить, если она назначена виртуальной машине.

Как создать группу безопасности

1. На экране **Группы безопасности** нажмите **Добавить группу безопасности**.
2. В окне **Добавить группу безопасности** введите имя и описание для группы и нажмите

Добавить.



По умолчанию новая группа безопасности будет отклонять весь входящий трафик и разрешать только исходящий трафик для назначенных виртуальных машин.

Как удалить группу безопасности

1. На экране **Группы безопасности** щелкните по нужной группе.
2. На правой панели группы нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

5.2.2 Управление правилами групп безопасности

Группы безопасности можно изменять путем добавления и удаления правил. Редактирование правил не предусмотрено. Если необходимо изменить существующее правило, удалите его и создайте заново с нужными параметрами.

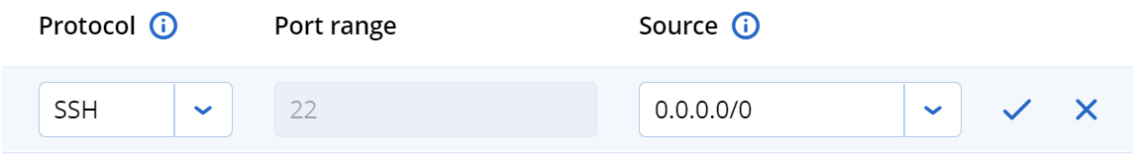
Предварительные требования

- Создана группа безопасности, как описано в разделе "Создание и удаление групп безопасности" (стр. 39).

Как добавить правило в группу безопасности

1. На экране **Группы безопасности** щелкните по группе, в которую следует добавить правило.
2. На правой панели группы нажмите **Добавить** в разделе **Входящие** или **Исходящие**, чтобы создать правило для входящего или исходящего трафика.
3. Укажите параметры правила.
   a. Выберите протокол из списка или введите число от 0 до 255.
   b. Введите номер порта или диапазон номеров. У некоторых протоколов уже есть стандартный диапазон портов. Например, для SSH используется порт 22.

c. Выберите готовую маску подсети (CIDR) или существующую группу безопасности.



4. Щелкните по галочке, чтобы сохранить изменения.

Сразу после создания правило применяется ко всем виртуальным машинам, назначенным в эту группу безопасности.

Как удалить правило из группы безопасности

1. На экране **Группы безопасности** щелкните по нужной группе.
2. На правой панели группы щелкните по значку корзины рядом с правилом, которое следует удалить.

Сразу после удаления правила это изменение применяется ко всем виртуальным машинам, назначенным в эту группу безопасности.

5.2.3 Изменение назначения групп безопасности

При создании ВМ выбираются группы безопасности для сетевых интерфейсов ВМ. Назначенные группы безопасности можно изменить позже.

Ограничения

- Нельзя настроить группы безопасности, если для выбранной сети отключена защита от спуфинга или отключено управление IP-адресами.

Как просмотреть виртуальные машины, назначенные в группу безопасности

1. На экране **Группы безопасности** щелкните по нужной группе.
2. На правой панели группы перейдите на вкладку **Назначенные ВМ**. Отобразятся все назначенные виртуальные машины и их статусы.

Можно щелкнуть по имени ВМ, чтобы открыть панель **Сводка** этой ВМ и изменить назначенную группу безопасности для ее сетевых интерфейсов.

Как назначить группу безопасности виртуальной машине

1. На экране **Виртуальные машины** щелкните по нужной ВМ.
2. На вкладке **Сводка** щелкните по значку карандаша в разделе **Сети**.
3. Щелкните по значку многоточия рядом с сетевым интерфейсом, которому следует назначить группу безопасности, и выберите **Изменить**.
4. В окне **Изменить сетевой интерфейс** перейдите на вкладку **Группы безопасности**.
5. Выберите одну или несколько групп безопасности из раскрывающегося списка и нажмите **Сохранить**.

Правила из выбранных групп безопасности будут применены во время выполнения.

5.3 Управление кластерами Kubernetes

Пользователи в режиме самообслуживания могут развертывать готовые кластеры Kubernetes с постоянным хранилищем для управления контейнерными приложениями.

Кластер Kubernetes включает следующие компоненты:

Компонент	Название и версия
Базовая ОС	Fedora 34 CoreOS
Среда выполнения контейнеров	Docker 20.10.6
Подключаемый сетевой модуль	Flannel с VXLAN

Ограничения

- Версии Kubernetes 1.15.x, 1.18.x и 1.19.x больше не поддерживаются. Кластеры Kubernetes, созданные в этих версиях, имеют метку **Устаревший**.
- Сертификаты кластеров Kubernetes выпускаются со сроком действия один год. Чтобы продлить сертификаты, используйте утилиту kubeadm, как описано в официальной документации.

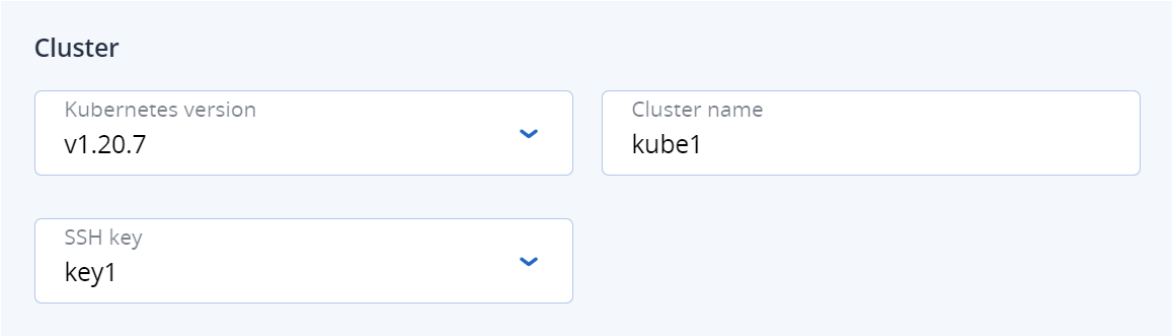
5.3.1 Создание и удаление кластеров Kubernetes

Предварительные требования

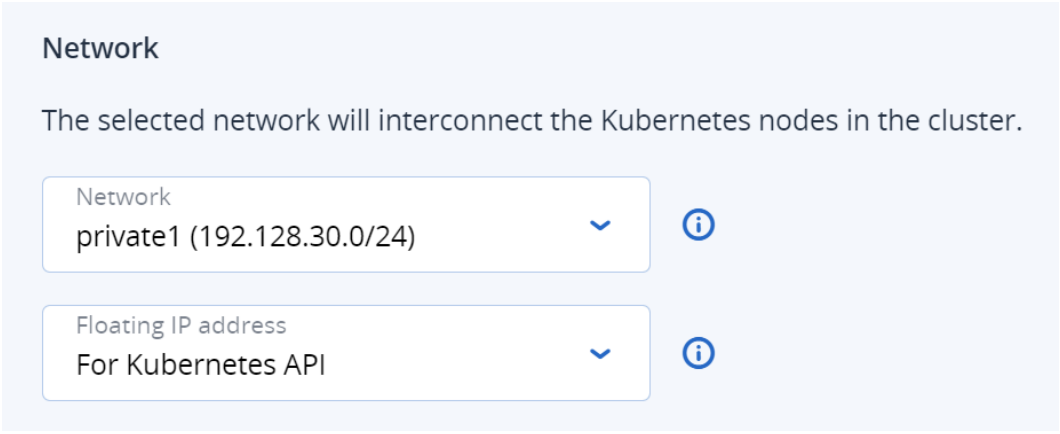
- Компонент «Kubernetes как услуга» должен быть установлен системным администратором. Его можно развернуть одновременно с вычислительным кластером или позже.
- Имеется сеть, которая будет связывать мастер-серверы и рабочие серверы Kubernetes. Это может быть либо общая физическая сеть, либо виртуальная сеть, соединенная с физической через виртуальный маршрутизатор. Для этой виртуальной сети должны быть указаны шлюз и DNS-сервер.
- Добавлен SSH-ключ, который будет установлен на рабочих и мастер-серверах.
- Достаточное количество ресурсов для всех серверов Kubernetes с учетом их типов.
- Также необходимо, чтобы сеть, в которой создается кластер Kubernetes, не накладывалась на эти стандартные сети:
  - 10.100.0.0/24 – используется для сетевого взаимодействия на уровне подов.
  - 10.254.0.0/16 – используется для назначения IP-адресов кластера Kubernetes.

Как создать кластер Kubernetes

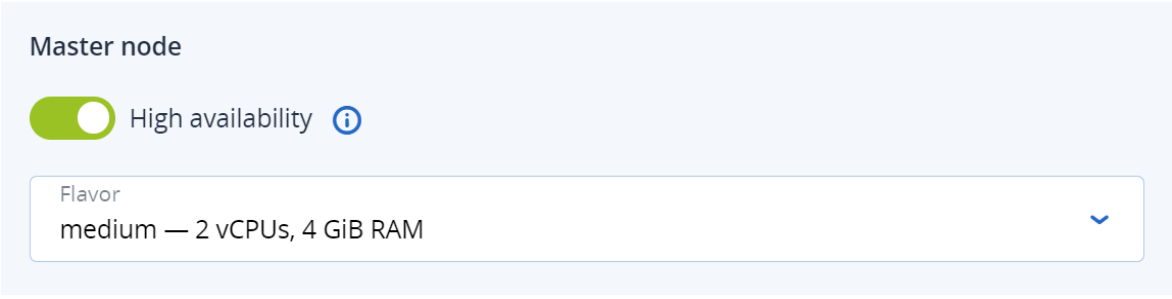
1. Перейдите на экран **Кластеры Kubernetes** и нажмите кнопку **Создать** справа. Откроется окно, в котором можно задать параметры кластера.
2. В разделе **Кластер** выберите версию Kubernetes, введите имя кластера и выберите SSH-ключ.



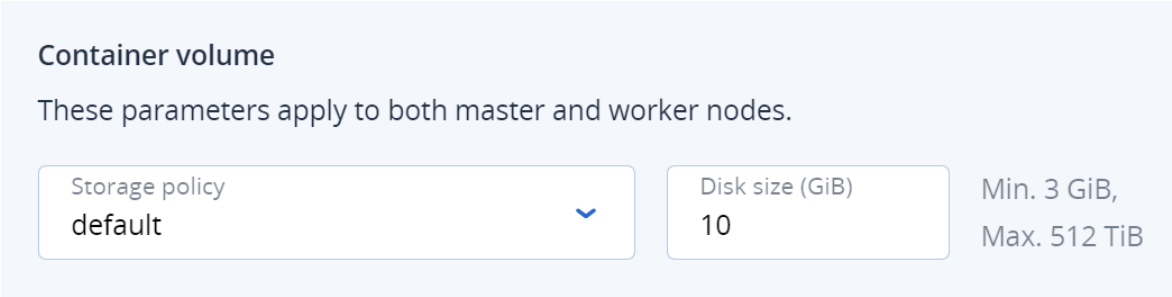
3. В разделе **Сеть** выберите сеть, которая будет соединять серверы Kubernetes в кластере. При выборе виртуальной сети следует решить, нужен ли доступ к кластеру Kubernetes через плавающий IP-адрес.
   - Если выбрать **Нет**, у вас не будет доступа к API Kubernetes.
   - Если выбрать **Для API Kubernetes**, плавающий IP-адрес будет назначен мастер-серверу или балансировщику нагрузки, если это мастер-сервер с высокой доступностью.
   - Если выбрать **Для API и серверов Kubernetes**, плавающие IP-адреса будут дополнительно назначены всем серверам Kubernetes (рабочим и мастер-серверам).



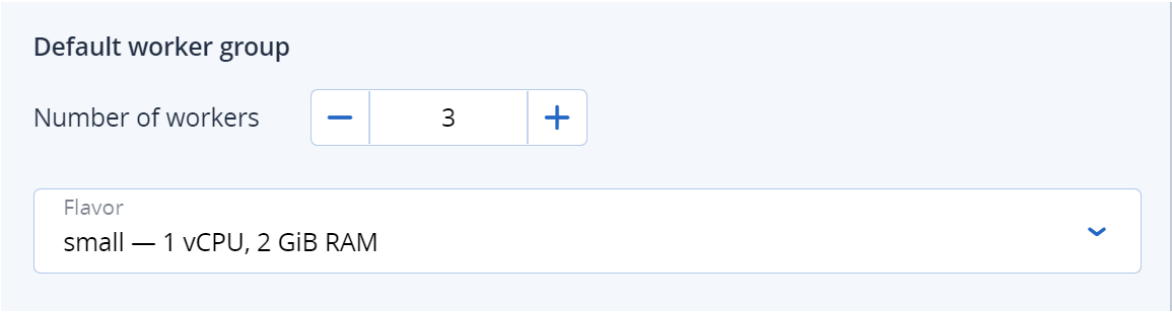
4. В разделе **Мастер-сервер** выберите тип ВМ и укажите, следует ли включить высокую доступность для мастер-сервера. Если включить высокую доступность, будет создано три экземпляра мастер-сервера. Они будут работать в режиме Active/Active.



5. В разделе **Том контейнера** выберите политику хранилища и введите размер для томов на рабочих и мастер-серверах.



6. В разделе **Рабочая группа по умолчанию** укажите количество создаваемых рабочих серверов и выберите тип ВМ для каждого из них.



7. Нажмите кнопку **Создать**.

Начнется создание кластера Kubernetes. Мастер-серверы и рабочие серверы появятся на странице **Виртуальные машины**, а их тома отобразятся на странице **Тома**.

Когда кластер будет готов, нажмите **Доступ к Kubernetes**, чтобы получить инструкции для доступа к панели мониторинга.

Как удалить кластер Kubernetes

Щелкните по нужному кластеру Kubernetes на экране **Кластеры Kubernetes** и нажмите **Удалить**. Рабочие и мастер-ВМ будут удалены вместе со своими томами.

5.3.2 Управление группами рабочих серверов Kubernetes

Для соответствия системным требованиям приложений, работающих в кластерах Kubernetes, можно использовать рабочие серверы с разным количеством ЦП и объемом ОЗУ. Создание рабочих серверов с разными типами ВМ возможно с помощью рабочих групп.

При создании кластера Kubernetes можно задать конфигурацию только одной группы рабочих серверов – группы по умолчанию. После создания кластера можно добавить любое количество групп. Кроме того, при необходимости можно позже изменить число рабочих серверов в группе.

Ограничения

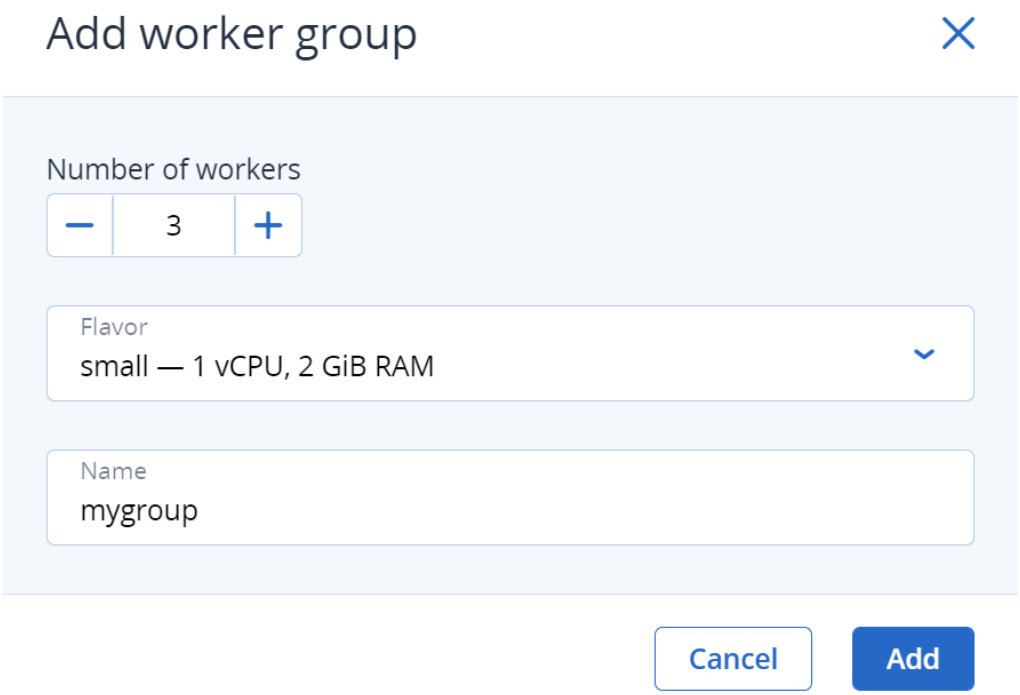
- Группы рабочих серверов недоступны в Kubernetes версии 1.15.x.
- Только пользователь, создавший кластер Kubernetes, может изменять его рабочие группы.
- Нельзя удалить группу рабочих серверов по умолчанию.

Предварительные требования

- Создан кластер Kubernetes, как описано в разделе "Создание и удаление кластеров Kubernetes" (стр. 42).

Как добавить группу рабочих серверов

1. На экране **Кластеры Kubernetes** щелкните по кластеру.
2. На правой панели кластера перейдите на вкладку **Группы**.
3. В разделе **Рабочие** нажмите **Добавить**.
4. В окне **Добавить рабочую группу** задайте число создаваемых рабочих серверов, выберите для каждого тип ВМ, а также укажите имя группы. Затем нажмите **Добавить**.



После создания группы рабочих серверов можно назначить поды на эти серверы, как описано в разделе "Назначение подов Kubernetes на определенные серверы" (стр. 55).

Как изменить число рабочих серверов в группе

1. На правой панели кластера Kubernetes перейдите на вкладку **Группы**.
2. В разделе **Рабочие** щелкните по значку карандаша для рабочей группы по умолчанию или значку многоточия для всех остальных групп и выберите **Изменить**.
3. В окне **Изменить рабочую группу** измените число рабочих серверов и нажмите **Сохранить**.

Как удалить группу рабочих серверов

Щелкните по значку многоточия рядом с нужной рабочей группой и выберите **Удалить**. Группа будет удалена вместе со всеми ее рабочими серверами. После удаления данные рабочей группы будут потеряны.

5.3.3 Обновление кластеров Kubernetes

Когда становится доступна новая версия Kubernetes, можно обновить свой кластер Kubernetes до этой версии. Обновление не прерывает работу серверов Kubernetes, поскольку они обновляются по очереди с сохранением доступности данных. API-интерфейс Kubernetes будет недоступен во время обновления, если для мастер-сервера не включена высокая доступность.

Ограничения

- Нельзя обновить кластеры Kubernetes версии 1.15.x. до более новых версий.
- Во время обновления нельзя управлять кластерами Kubernetes на панели самообслуживания.

Предварительные требования

- Создан кластер Kubernetes, как описано в разделе "Создание и удаление кластеров Kubernetes" (стр. 42).

Как обновить кластер Kubernetes

1. Щелкните по кластеру Kubernetes с отметкой **Доступно обновление**.
2. На правой панели кластера нажмите **Обновить** в поле **Версия Kubernetes**.
3. В окне **Обновить** выберите версию Kubernetes, до которой следует выполнить обновление, и перейдите по предоставленной ссылке, чтобы прочитать сведения о ресурсах API, которые устарели или больше не поддерживаются в выбранной версии. Затем нажмите **Обновить**.
4. В окне подтверждения нажмите **Подтвердить**.

Предупреждение
Не выполняйте управление виртуальными машинами Kubernetes во время обновления, поскольку это может привести к прерыванию процесса обновления и неработоспособности кластера.

5.3.4 Использование постоянных томов для подов Kubernetes

Kubernetes позволяет использовать вычислительные тома в качестве постоянного хранилища для подов. Постоянные тома (Persistent Volumes, PV) существуют независимо от подов. Это означает, что такой том продолжает существовать после удаления пода, к которому он был подключен. Этот PV можно подключить к другим подам для доступа к хранящимся на нем данным. Можно применять динамическое выделение постоянных томов без необходимости их создания вручную либо статическое, используя тома, существующие в вычислительном кластере.

5.3.4.1 Создание классов хранилищ

В продукте Кибер Инфраструктура классы хранилища соответствуют политикам вычислительного хранилища, определенным на панели администрирования. Создание класса хранилища требуется для всех операций с хранилищем в кластере Kubernetes.

Как создать класс хранилища

Нажмите **+ Создать** на панели мониторинга Kubernetes и укажите YAML-файл, который определяет этот объект, например:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
 name: mysc
provisioner: cinder.csi.openstack.org
parameters:
 type: default
```

Этот манифест описывает класс хранилища mysc с политикой default. Политика хранилища должна существовать в вычислительном кластере и быть указана в квотах хранения для текущего проекта.

5.3.4.2 Динамическое выделение постоянных томов

Постоянные тома могут динамически выделяться посредством запросов на хранилище (Persistent Volume Claims, PVC). PVC запрашивает PV с определенным классом хранилища, режимом доступа и размером. Если подходящий PV существует в кластере, он привязывается к запросу. Если подходящих PV нет, но их можно выделить, то создается новый том и привязывается к запросу. Kubernetes использует PVC для получения зарезервированного PV и подключает его к поду.

Предварительные требования

- Под и используемый им запрос постоянного тома должны находиться в одном пространстве имен.

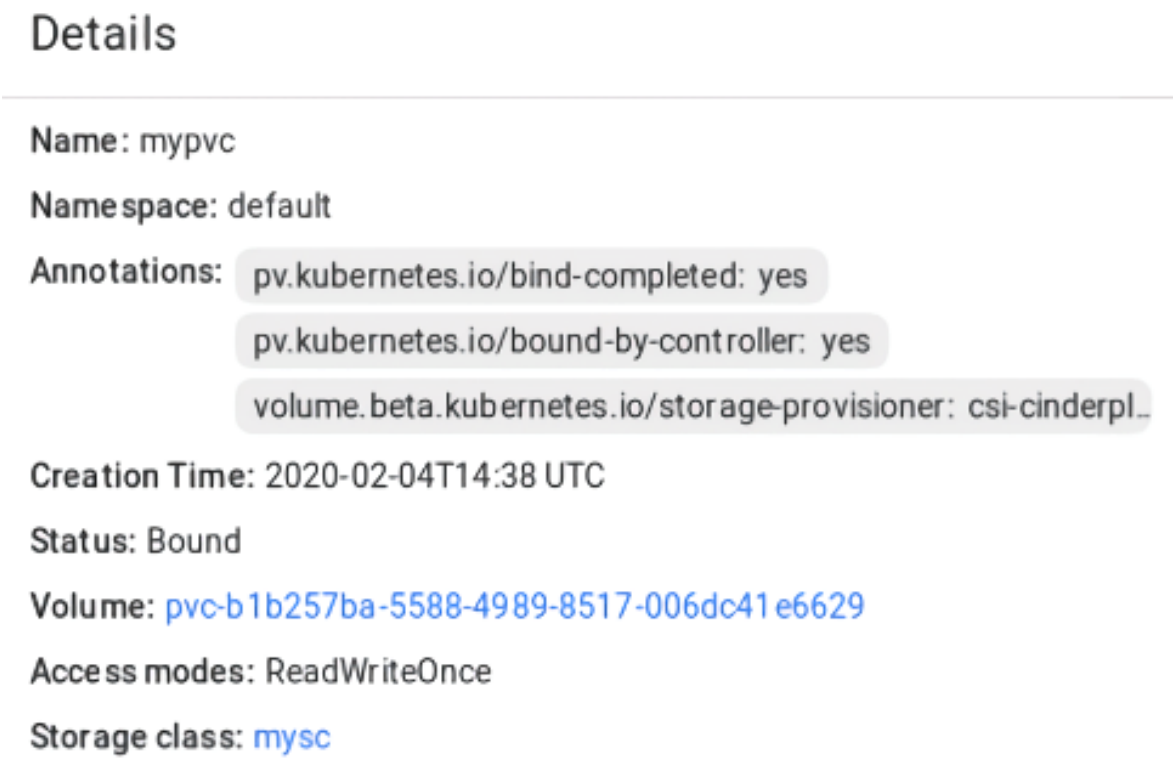
Как динамически выделить PV для пода

1. Выполните доступ к кластеру Kubernetes через панель мониторинга. Нажмите **Доступ к Kubernetes** для получения инструкций.
2. На панели мониторинга Kubernetes создайте класс хранилища, как описано в разделе "Создание классов хранилищ" (стр. 46).
3. Создайте запрос постоянного тома. Для этого нажмите **+ Создать** и укажите следующий YAML-файл:

   ```
   apiVersion: v1
   kind: PersistentVolumeClaim
   metadata:
    name: mypvc
   spec:
    accessModes:
    - ReadWriteOnce
    resources:
     requests:
       storage: 10Gi
    storageClassName: mysc
   ```

Этот манифест описывает запрос постоянного тома mypvc, который запрашивает из класса хранилища mysc том размером не менее 10 ГиБ, который можно подключить в режиме чтения/записи к одному серверу.

Создание PVC запускает динамическое выделение постоянного тома, который соответствует требованиям запроса. Затем Kubernetes привязывает том к запросу.



4. Создайте под и укажите PVC в качестве его тома. Для этого нажмите **+ Создать** и введите следующий YAML-файл:

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
spec:
  containers:
  - image: nginx
    imagePullPolicy: IfNotPresent
    name: nginx
    ports:
    - containerPort: 80
      protocol: TCP
    volumeMounts:
      - mountPath: /var/lib/www/html
        name: mydisk
  volumes:
  - name: mydisk
    persistentVolumeClaim:
```

```
claimName: mypvc
readOnly: false
```

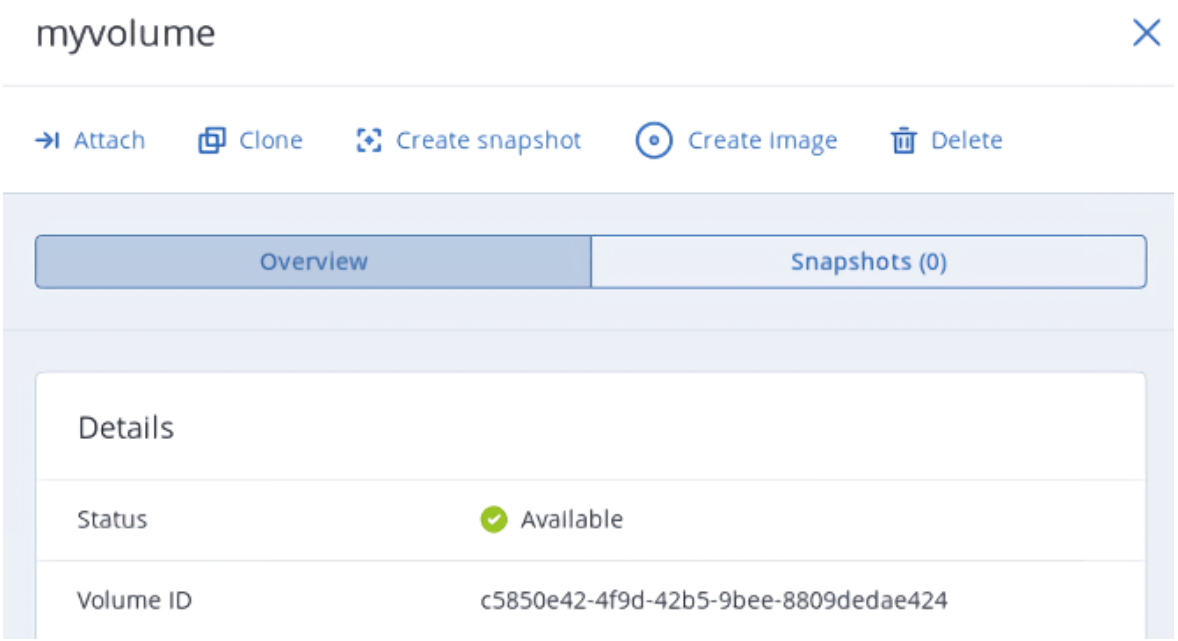
Этот файл конфигурации описывает под nginx, который использует запрос постоянного тома mypvc. Постоянный том, привязанный к запросу, будет доступен по адресу /var/lib/www/html внутри контейнера nginx.

5.3.4.3 Статическое выделение постоянных томов

Можно подключать к подам существующие вычислительные тома с помощью статического выделения постоянных томов.

Как подключить вычислительный том

1. На панели самообслуживания получите идентификатор нужного тома.



2. Выполните доступ к кластеру Kubernetes через панель мониторинга. Нажмите **Доступ к Kubernetes** для получения инструкций.
3. На панели мониторинга Kubernetes создайте класс хранилища, как описано в разделе "Создание классов хранилищ" (стр. 46).
4. Создайте постоянный том. Для этого нажмите **+ Создать** и укажите следующий YAML-файл:

```
apiVersion: v1
kind: PersistentVolume
metadata:
 annotations:
   pv.kubernetes.io/provisioned-by: cinder.csi.openstack.org
 name: mypv
spec:
 accessModes:
```

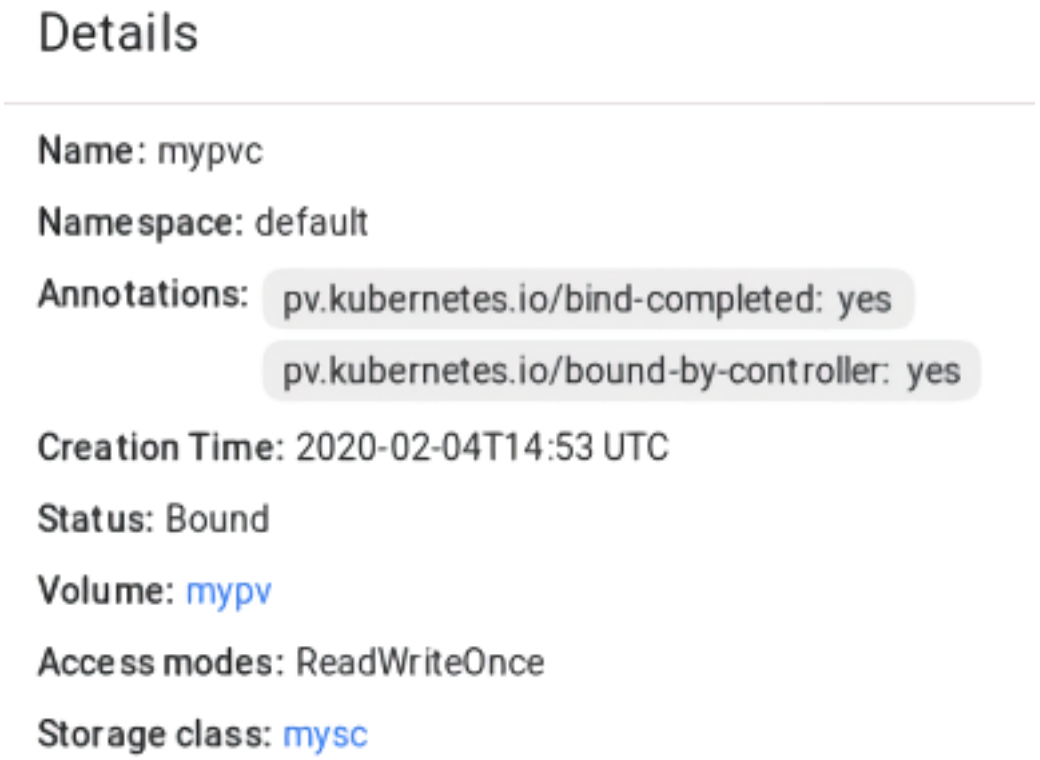
```
  - ReadWriteOnce
  capacity:
    storage: 10Gi
  csi:
    driver: cinder.csi.openstack.org
    fsType: ext4
    volumeHandle: c5850e42-4f9d-42b5-9bee-8809dedae424
  persistentVolumeReclaimPolicy: Delete
  storageClassName: mysc
```

Этот манифест описывает постоянный том mypv из класса хранилища mysc размером 10 ГиБ, который можно подключить в режиме чтения/записи к одному серверу. PV mypv использует вычислительный том с идентификатором c5850e42-4f9d-42b5-9bee-8809dedae424 в качестве внешнего хранилища.

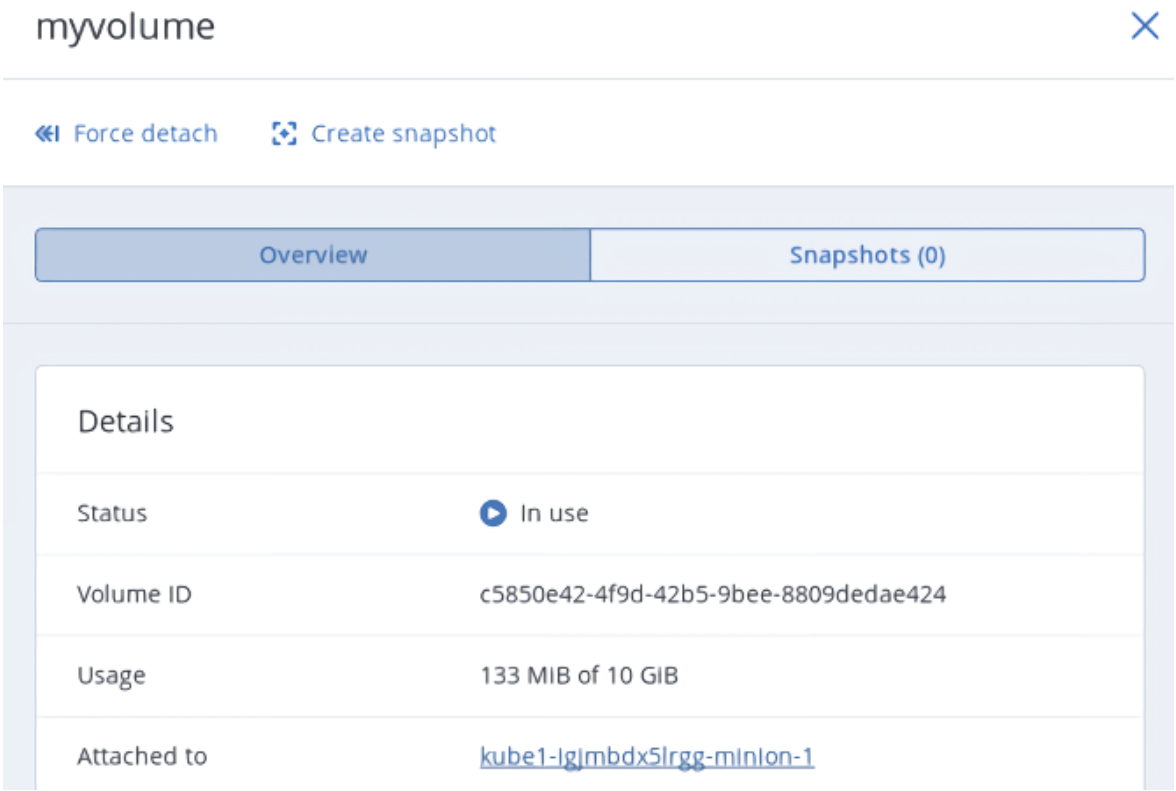
5. Создайте запрос постоянного тома. Перед тем как определить параметры PVC, убедитесь, что нужный PV создан и имеет статус «Доступен». Существующий PV должен соответствовать требованиям запроса относительно размера, режима доступа и класса хранилища. Нажмите **+ Создать** и укажите следующий YAML-файл:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mypvc
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 10Gi
  storageClassName: mysc
```

После создания запроса постоянного тома mypvc к нему привязывается том mypv.



6. Создайте под и укажите PVC в качестве его тома. Используйте пример из шага 4 в разделе "Динамическое выделение постоянных томов" (стр. 47).
   На панели самообслуживания вычислительный том будет подключен к виртуальной машине, на которой работает этот под Kubernetes.



5.3.4.4 Обеспечение высокой доступности развертываний Kubernetes

Если сервер, на котором размещен под Kubernetes, выйдет из строя или станет недоступен по сети, под зависнет в переходном состоянии. В этом случае постоянные тома пода не отсоединяются автоматически, что не дает заново развернуть под на другом рабочем сервере. Чтобы обеспечить высокую доступность приложений Kubernetes, необходимо настроить принудительное удаление пода в случае сбоя сервера путем добавления правил в развертывание пода.

Как удалить зависший под

Добавьте следующие строки в раздел spec файла конфигурации развертывания:

```
terminationGracePeriodSeconds: 0
tolerations:
- effect: NoExecute
key: node.kubernetes.io/unreachable
operator: Exists
tolerationSeconds: 2
- effect: NoExecute
key: node.kubernetes.io/not-ready
operator: Exists
tolerationSeconds: 2
```

Если состояние сервера меняется на «Не готов» или «Недоступен», под будет автоматически удален через 2 секунды.

Полный YAML-файл развертывания может выглядеть следующим образом.

```
apiVersion: apps/v1
kind: Deployment
metadata:
 name: nginx
spec:
 replicas: 1
 selector:
  matchLabels:
   app: nginx
 template:
  metadata:
   labels:
    app: nginx
  spec:
   terminationGracePeriodSeconds: 0
   tolerations:
   - effect: NoExecute
    key: node.kubernetes.io/unreachable
    operator: Exists
    tolerationSeconds: 2
   - effect: NoExecute
```

```
    key: node.kubernetes.io/not-ready
    operator: Exists
    tolerationSeconds: 2
  containers:
  - image: nginx
    imagePullPolicy: IfNotPresent
    name: nginx
    ports:
    - containerPort: 80
      protocol: TCP
    volumeMounts:
      - mountPath: /var/lib/www/html
        name: mydisk
  volumes:
    - name: mydisk
      persistentVolumeClaim:
        claimName: mypvc
```

Приведенный выше манифест описывает развертывание nginx с одним подом, который использует запрос постоянного тома mypvc и будет автоматически удален через 2 секунды в случае сбоя сервера.

5.3.5 Создание внешних балансировщиков нагрузки в Kubernetes

В Kubernetes можно создать сервис с внешним балансировщиком нагрузки, который обеспечивает доступ к системе из внешних сетей. Балансировщик нагрузки получает публично доступный IP-адрес и перенаправляет входящие запросы на нужный порт на серверах кластера Kubernetes.

Как создать сервис с внешним балансировщиком нагрузки

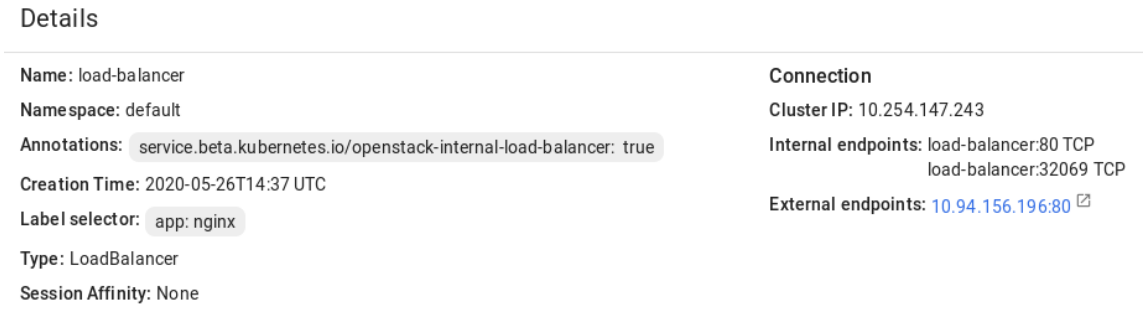
1. Выполните доступ к кластеру Kubernetes через панель мониторинга. Нажмите **Доступ к Kubernetes** для получения инструкций.
2. На панели мониторинга Kubernetes создайте развертывание и сервис типа **LoadBalancer**. Для этого нажмите **+ Создать** и укажите YAML-файл, который определяет эти объекты, например:
   - Если ваш кластер Kubernetes развернут в общей физической сети, укажите следующий манифест:

     ```
     apiVersion: apps/v1
     kind: Deployment
     metadata:
       name: nginx
     spec:
       replicas: 2
       selector:
         matchLabels:
           app: nginx
       template:
         metadata:
           labels:
             app: nginx
     ```

```
    spec:
      containers:
      - name: nginx
        image: nginx
        ports:
        - containerPort: 80
---
kind: Service
apiVersion: v1
metadata:
  name: load-balancer
  annotations:
    service.beta.kubernetes.io/openstack-internal-load-balancer: "true"
spec:
  selector:
    app: nginx
  type: LoadBalancer
  ports:
  - port: 80
    targetPort: 80
    protocol: TCP
```

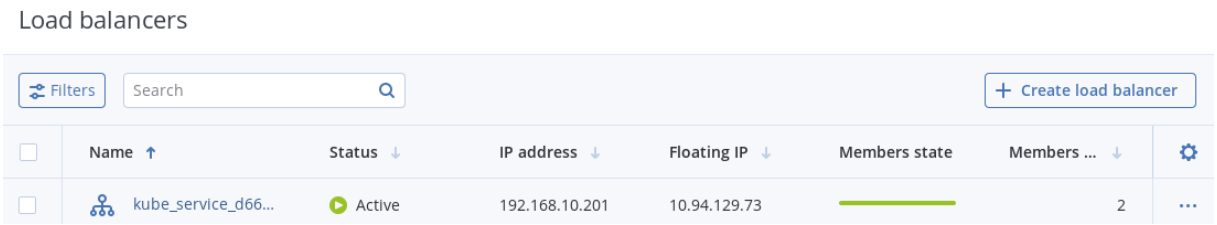
Приведенный выше манифест описывает развертывание nginx с набором реплик из двух подов и сервис load-balancer типа LoadBalancer. Аннотация, используемая для сервиса, указывает, что балансировщик нагрузки будет внутренним.

После создания балансировщик нагрузки получит IP-адрес из общей физической сети и будет доступен на этой внешней оконечной точке.



- Если ваш кластер Kubernetes развернут в виртуальной сети, соединенной с физической сетью через виртуальный маршрутизатор, можно использовать приведенный выше YAML-файл без раздела annotations для сервиса load-balancer. Созданный балансировщик нагрузки получит плавающий IP-адрес из физической сети и будет доступен на этой внешней оконечной точке.

Балансировщик нагрузки также появится на панели самообслуживания, где можно отслеживать его состояние и производительность, например:



5.3.6 Назначение подов Kubernetes на определенные серверы

Используя группы рабочих серверов, можно назначить под в Kubernetes на определенные серверы. При создании пользовательской рабочей группы к ее серверам добавляется метка с именем группы. Если вы хотите назначить под на сервер из определенной рабочей группы, добавьте раздел выбора сервера с меткой группы в файл конфигурации пода.

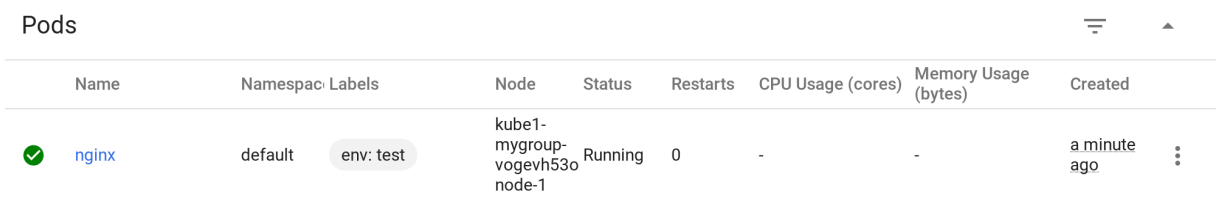
Как создать под, который будет назначен на определенный сервер

Нажмите **+ Создать** на панели мониторинга Kubernetes и укажите YAML-файл, который определяет этот объект, например:

```
apiVersion: v1
kind: Pod
metadata:
 name: nginx
 labels:
  env: test
spec:
 containers:
 - name: nginx
  image: nginx
  imagePullPolicy: IfNotPresent
 nodeSelector:
  magnum.openstack.org/nodegroup: mygroup
```

Этот манифест описывает под nginx, который будет назначен на сервер из группы mygroup.

После создания пода проверьте, что сервер размещения принадлежит к указанной группе рабочих серверов.



5.4 Управление образами

Кибер Инфраструктура позволяет загружать ISO-образы и шаблоны, которые можно использовать для создания томов ВМ.

- ISO-образ – это стандартный формат дистрибутивов ОС, которые необходимо устанавливать на диск. ISO-образ можно загрузить в вычислительный кластер.
- Шаблон – это готовый загрузочный том в формате QCOW2 с установленной операционной системой и приложениями. Многие поставщики ОС предлагают шаблоны своих операционных систем, называя их облачными образами. Облачный образ можно загрузить из официального репозитория ОС, также можно подготовить собственный шаблон в вычислительном кластере.

Предварительные требования

- Знакомство с поддерживаемыми операционными системами, перечисленными в разделе "Поддерживаемые гостевые операционные системы" (стр. 16).

5.4.1 Загрузка образов

Как загрузить образ

1. На экране **Образы** нажмите **Добавить образ**.
2. В окне **Добавить образ** выполните следующие действия.
   a. Нажмите **Обзор** и выберите файл в одном из поддерживаемых форматов: .iso, .img, .qcow2, .raw.
   b. Укажите имя образа, которое будет отображаться на панели администратора.
   c. Выберите правильный тип ОС из раскрывающегося списка.

   Внимание
   Тип ОС влияет на параметры ВМ, такие как настройки гипервизора. ВМ, созданные из образа с неверным типом ОС, могут работать неправильно, например могут происходить сбои.

3. Нажмите **Добавить**, чтобы начать передачу образа. Индикатор хода загрузки будет отображаться в правом нижнем углу.

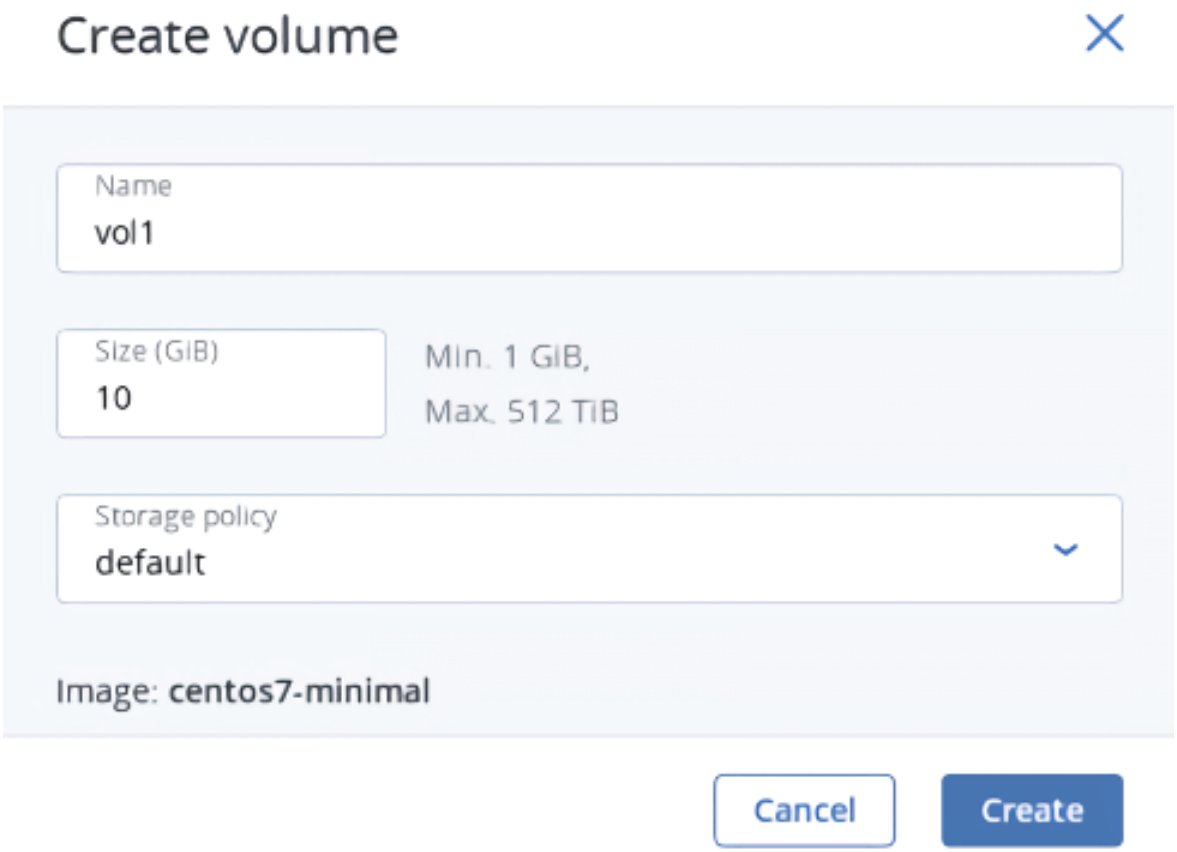
Всплывающее окно можно скрыть, не прерывая процесса загрузки. Индикатор хода загрузки будет доступен в центре уведомлений.

5.4.2 Создание томов из образов

Тома можно создавать как из ISO-образов, так и из шаблонов.

Как создать том из образа

1. Перейдите на экран **Образы** и щелкните по нужному образу.
2. На панели образа нажмите **Создать том**.
3. В окне **Создать том** укажите имя и размер тома и выберите политику хранилища.



4. Нажмите кнопку **Создать**.

Новый том появится на экране **Тома**.

5.4.3 Подготовка шаблонов

Создание шаблона может потребоваться в следующих случаях:

- Аварийное восстановление виртуальной машины.
- Создание ВМ, доступной через SSH.
- Создание ВМ, настраиваемой с пользовательскими данными.

Общая схема подготовки

1. Установите Cloudbase-Init и OpenSSH Server в виртуальную машину.
2. [Необязательно] Включите ведение журнала для виртуальных машин, которые будут создаваться из шаблона.
3. Преобразуйте загрузочный том ВМ в шаблон, как описано в разделе "Создание образов из томов" (стр. 66).

5.4.3.1 Подготовка шаблонов Linux

Поскольку во всех гостевых ОС Linux по умолчанию предустановлен OpenSSH Server, необходимо только убедиться, что в шаблоне Linux установлен пакет cloud-init.

Самый простой способ получить шаблон Linux с установленным пакетом cloud-init – загрузить из официального репозитория. Либо можно создать шаблон Linux из существующего загрузочного тома.

5.4.3.2 Подготовка шаблонов Windows

В гостевых ОС Windows по умолчанию не предустановлены ни Cloudbase-Init, ни OpenSSH Server. Их необходимо установить и настроить вручную.

Как установить Cloudbase-Init и OpenSSH Server в виртуальную машину Windows

1. Выполните вход в ВМ Windows.
2. Создайте новую учетную запись администратора, которая будет использоваться для SSH-подключений, и выполните вход с этой учетной записью.
3. Чтобы установить и настроить OpenSSH Server
   a. Запустите Windows PowerShell с правами администратора и установите для политики выполнения значение Unrestricted, чтобы иметь возможность выполнять скрипты.

      ```
      > Set-ExecutionPolicy Unrestricted
      ```

   b. Загрузите OpenSSH Server (например, из репозитория GitHub), распакуйте архив в папку C:\Program Files и установите его, выполнив следующую команду:

      ```
      > & 'C:\Program Files\OpenSSH-Win64\install-sshd.ps1'
      ```

   c. Запустите сервис sshd и задайте для него автоматический тип запуска.

      ```
      > net start sshd
      > Set-Service sshd -StartupType Automatic
      ```

   d. Откройте порт TCP 22 для сервиса OpenSSH в брандмауэре Windows.
      - В Windows 8.1, Windows Server 2012 и более новых версиях выполните следующую команду:

        ```
        > New-NetFirewallRule -Protocol TCP -LocalPort 22 -Direction Inbound -Action Allow -DisplayName OpenSSH
        ```

      - В Windows 7, Windows Server 2008 и Windows Server 2008 R2 выполните следующую команду:

        ```
        > netsh advfirewall firewall add rule name=sshd dir=in action=allow protocol=TCP localport=22
        ```

e. Откройте файл C:\ProgramData\ssh\sshd_config.

```
> notepad 'C:\ProgramData\ssh\sshd_config'
```

Закомментируйте следующие строки в конце файла:

```
#Match Group administrators
#AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

Сохраните изменения.

f. Создайте папку .ssh в C:\Users\<current_user> и пустой файл authorized_keys внутри нее.

```
> cd C:\Users\<current_user>
> mkdir .ssh
> notepad .\.ssh\authorized_keys
```

Удалите расширение .txt у созданного файла.

```
> move .\.ssh\authorized_keys.txt .\.ssh\authorized_keys
```

g. Измените разрешения для созданного файла, чтобы отключить наследование.

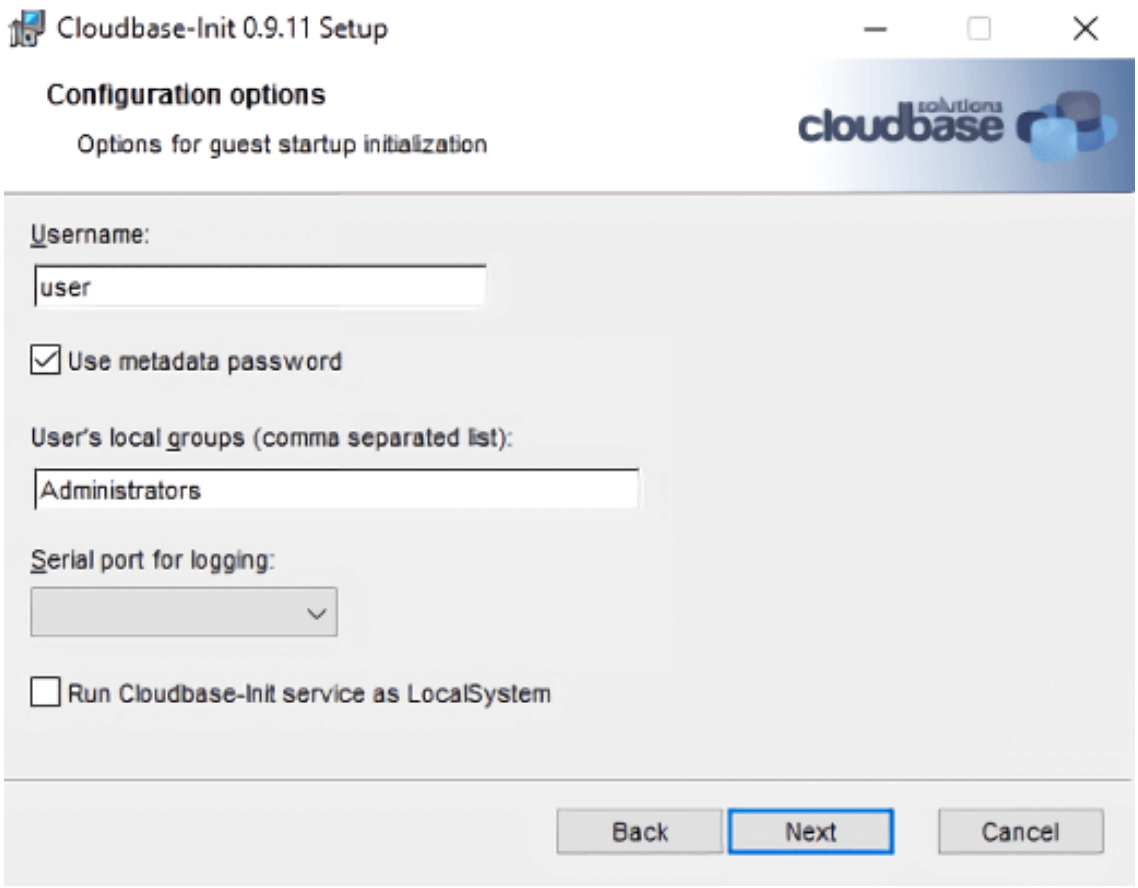
```
> icacls .\.ssh\authorized_keys /inheritance:r
```

4. Загрузите Cloudbase-Init (например, с официального сайта), запустите установку и следуйте инструкциям на экране.

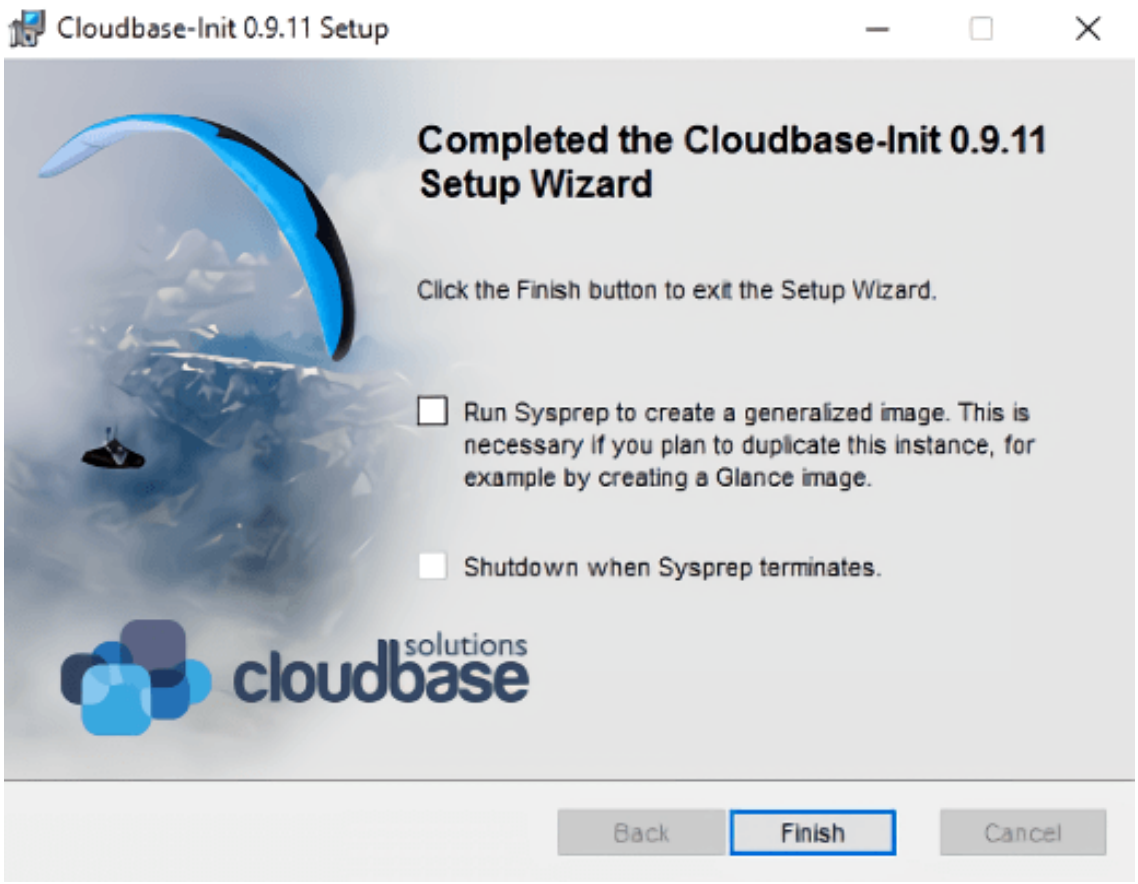
a. В окне **Параметры конфигурации** введите текущее имя пользователя в поле **Имя пользователя**.

Внимание

Пароль учетной записи будет сброшен при следующем запуске ВМ. Вы сможете выполнить вход с этой учетной записью, используя метод аутентификации с ключом, либо установить новый пароль с помощью скрипта настройки.



b. После окончания установки не запускайте Sysprep и нажмите **Завершить**.



c. Запустите Windows PowerShell с правами администратора и откройте файл C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf.

```
> notepad 'C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf'
```

Добавьте metadata_services и plugins в две строки.

```
metadata_services=\
cloudbaseinit.metadata.services.configdrive.ConfigDriveService,\
cloudbaseinit.metadata.services.httpservice.HttpService\
plugins=cloudbaseinit.plugins.common.mtu.MTUPlugin,\
cloudbaseinit.plugins.windows.ntpclient.NTPClientPlugin,\
cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin,\
cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,\
cloudbaseinit.plugins.common.networkconfig.NetworkConfigPlugin,\
cloudbaseinit.plugins.windows.licensing.WindowsLicensingPlugin,\
cloudbaseinit.plugins.common.sshpublickeys.SetUserSSHPublicKeysPlugin,\
cloudbaseinit.plugins.windows.extendvolumes.ExtendVolumesPlugin,\
cloudbaseinit.plugins.common.setuserpassword.SetUserPasswordPlugin,\
cloudbaseinit.plugins.common.userdata.UserDataPlugin,\
cloudbaseinit.plugins.windows.winrmlistener.ConfigWinRMListenerPlugin,\
cloudbaseinit.plugins.windows.winrmcertificateauth.\
ConfigWinRMCertificateAuthPlugin,\
cloudbaseinit.plugins.common.localscripts.LocalScriptsPlugin
```

Примечание
Не забудьте удалить все символы обратной косой черты в строках выше.

Сохраните изменения.

5.4.3.3 Включение ведения журнала для виртуальных машин

Журнал консоли виртуальной машины можно использовать для диагностики проблем с загрузкой. Журнал содержит сообщения, только если ведение журнала включено внутри ВМ, иначе журнал будет пустым.

Ведение журнала можно активировать, включив уровни ведения журнала TTY1 и TTYS0 в ВМ Linux или перенаправление на консоль сервисов аварийного управления (EMS) в ВМ Windows. Также можно включить ведение журнала состояния драйверов в ВМ Windows, чтобы просматривать список загруженных драйверов. Это может пригодиться для диагностики неисправного драйвера или долгого процесса загрузки.

Как включить ведение журнала TTY1 и TTYS0 в виртуальных машинах Linux

1. Добавьте строку GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0" в файл /etc/default/grub.
2. В зависимости от загрузчика выполните команду

   ```
   # grub-mkconfig -o /boot/grub/grub.cfg
   ```

   или

   ```
   # grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

3. Перезагрузите ВМ.

Как включить перенаправление на консоль EMS в виртуальных машинах Windows

1. Запустите **Windows PowerShell** с правами администратора.
2. В консоли PowerShell задайте COM-порт и скорость передачи данных для перенаправления на консоль EMS. Поскольку виртуальные машины Windows имеют только порт COM1 со скоростью передачи 9600 бит/с, выполните следующую команду:

   ```
   bcdedit /emssettings EMSPORT:1
   ```

3. Включите EMS для текущей загрузочной записи:

   ```
   bcdedit /ems on
   ```

Как включить ведение журнала состояния драйверов в виртуальных машинах Windows

1. Запустите программу **Конфигурация системы** с правами администратора.
2. В окне **Конфигурация системы** откройте вкладку **Загрузка** и установите флажки **Информация об ОС** и **Сделать эти параметры загрузки постоянными**.
3. Подтвердите изменения и перезапустите систему.

5.5 Управление томами

Том в продукте Кибер Инфраструктура представляет собой виртуальный дисковый накопитель, который можно присоединить к виртуальной машине. Целостность данных в томах обеспечивается в соответствии с режимом избыточности, указанным в политике хранилища.

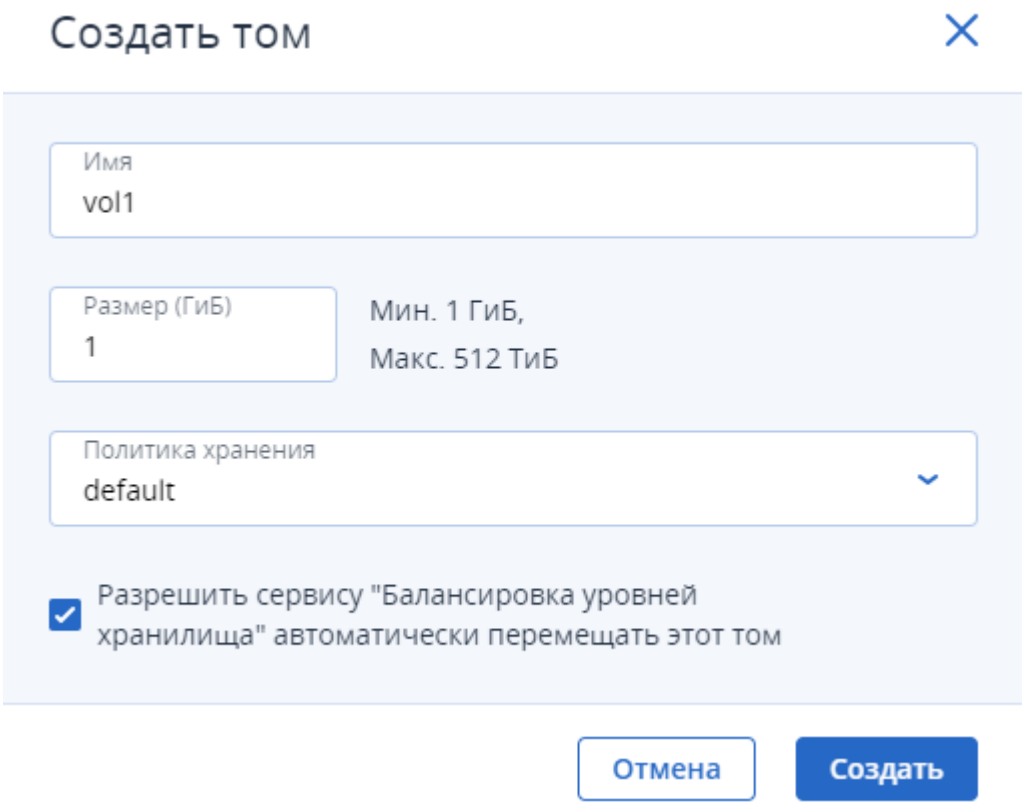
5.5.1 Создание и удаление томов

Ограничения

- Том удаляется вместе со всеми своими снимками.

Как создать том

1. На экране **Тома** нажмите **Создать том**.



2. В окне **Создать том** укажите имя и размер тома в гигабайтах, выберите политику хранилища. При необходимости снимите флажок **Разрешить сервису "Балансировка уровней хранилища" автоматически перемещать этот том**, который установлен по умолчанию.
3. Нажмите **Создать**.

Как удалить том

1. На вкладке **Тома** проверьте статус тома, который планируется удалить.
2. Если статус тома «Используется», щелкните по тому и нажмите **Отсоединить принудительно**.
3. Если статус тома «Доступен», щелкните по тому и нажмите **Удалить**.

5.5.2 Присоединение и отсоединение томов

Ограничения

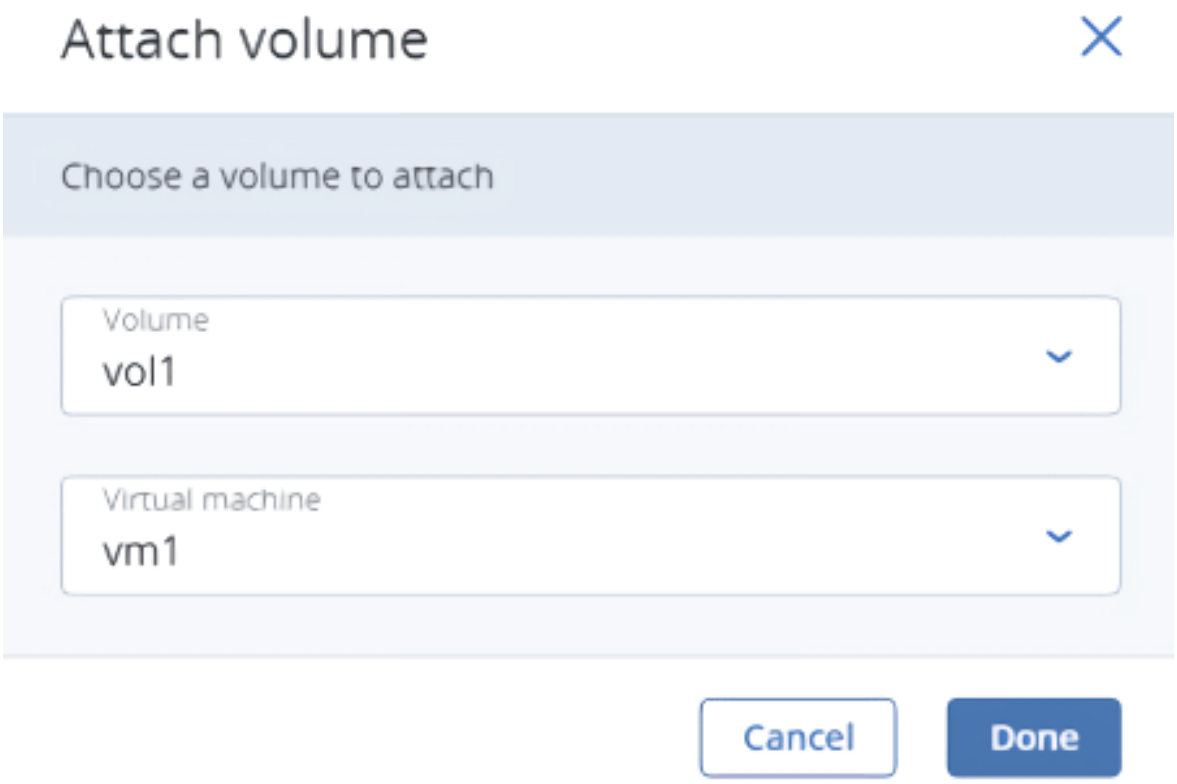
- Присоединять и отсоединять можно только незагрузочные тома.

Предварительные требования

- Создан том, как описано в разделе "Создание и удаление томов" (стр. 63).
- Чтобы можно было использовать тома, присоединенные к ВМ, они должны быть инициализированы внутри гостевой ОС стандартными средствами.

Как присоединить том к виртуальной машине

1. На экране **Тома** щелкните по неиспользуемому тому.
2. На правой панели тома нажмите **Присоединить**.
3. В окне **Присоединить том** выберите ВМ из раскрывающегося списка и нажмите **Готово**.



Как отсоединить том от виртуальной машины

1. На экране **Тома** щелкните по используемому тому.
2. Если ВМ остановлена, нажмите **Отсоединить** на правой панели тома.
3. Если ВМ работает, нажмите **Отсоединить принудительно** на правой панели тома.

Предупреждение
При этом есть риск потери данных.

5.5.3 Изменение размера томов

Размер томов можно изменять только в сторону увеличения. Тома можно расширять как для работающих (онлайн-режим), так и для остановленных (офлайн-режим) виртуальных машин. Изменение размера тома в онлайн-режиме позволяет избежать простоев и масштабировать емкость хранилища ВМ на лету без прерывания работы сервиса.

Ограничения

- Уменьшать размер томов нельзя.
- При изменении размера тома файловая система внутри гостевой ОС не расширяется.
- Если вернуть том к моментальному снимку, созданному до расширения, у тома останется новый размер.

Предварительные требования

- Создан том, как описано в разделе "Создание и удаление томов" (стр. 63).

Как увеличить размер тома

1. На экране **Тома** щелкните по тому.
2. Нажмите значок карандаша в поле **Размер**.
3. Введите нужную емкость тома и нажмите значок галочки.

После расширения тома потребуется заново создать разделы на диске внутри гостевой ОС, чтобы распределить добавленное дисковое пространство.

5.5.4 Изменение политики хранилища тома

Управлять избыточностью вычислительного тома можно путем изменения политики хранилища, примененной к этому тому. Политику хранилища можно изменять для томов, присоединенных как к работающим, так и остановленным виртуальным машинам.

Ограничения

- Для выбора будут доступны только политики хранилища, определенные квотами проекта.

Предварительные требования

- Создан том, как описано в разделе "Создание и удаление томов" (стр. 63).

Как изменить политику хранилища для тома

1. На экране **Тома** щелкните по тому.
2. Нажмите значок карандаша в поле **Политика хранения**.
3. Выберите новую политику хранилища и нажмите значок галочки. Можно выбрать только между политиками хранилища с одинаковым типом избыточности.

5.5.5 Создание образов из томов

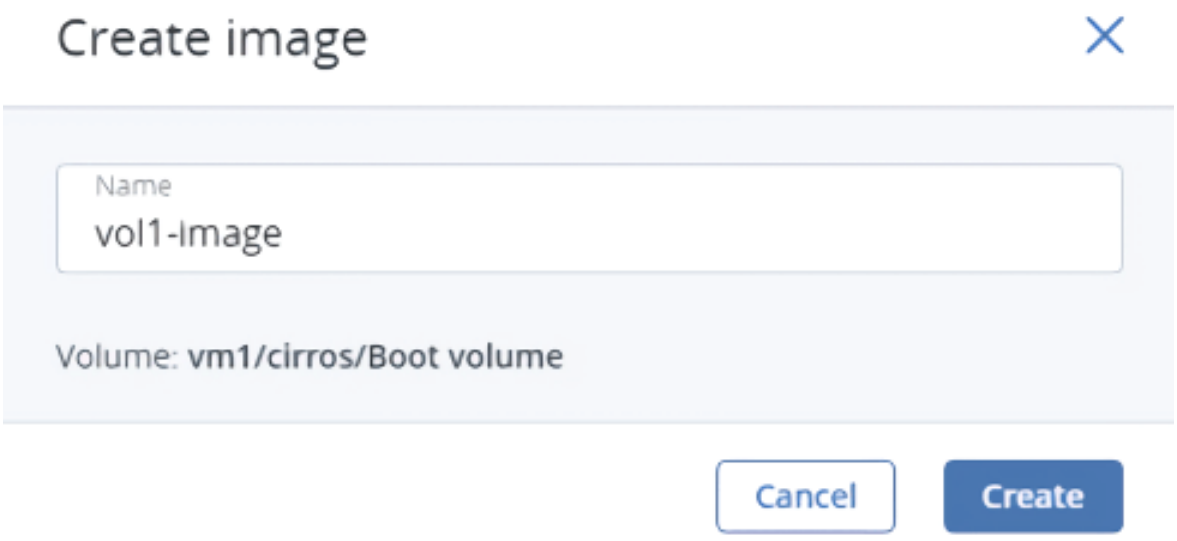
Чтобы создать несколько ВМ с одним и тем же загрузочным томом, можно создать образ на основе существующего загрузочного тома и развернуть из него виртуальные машины.

Предварительные требования

- На виртуальных машинах Linux должен быть установлен пакет cloud-init, как описано в разделе "Подготовка шаблонов Linux" (стр. 58).
- На виртуальных машинах Windows должны быть установлены Cloudbase-Init и OpenSSH Server, как описано в разделе "Подготовка шаблонов Windows" (стр. 58).
- [Необязательно] Ведение журнала должно быть включено внутри виртуальной машины, как указано в разделе "Включение ведения журнала для виртуальных машин" (стр. 62).

Как создать шаблон из загрузочного тома

1. Выключите ВМ, к которой присоединен исходный том.
2. Переключитесь на экран **Тома**, нажмите кнопку с многоточием в заголовке тома и выберите **Создать образ**.
3. В окне **Создать образ** введите имя образа и нажмите **Создать**.



Новый образ появится на экране **Образы**.

5.5.6 Клонирование томов

Ограничения

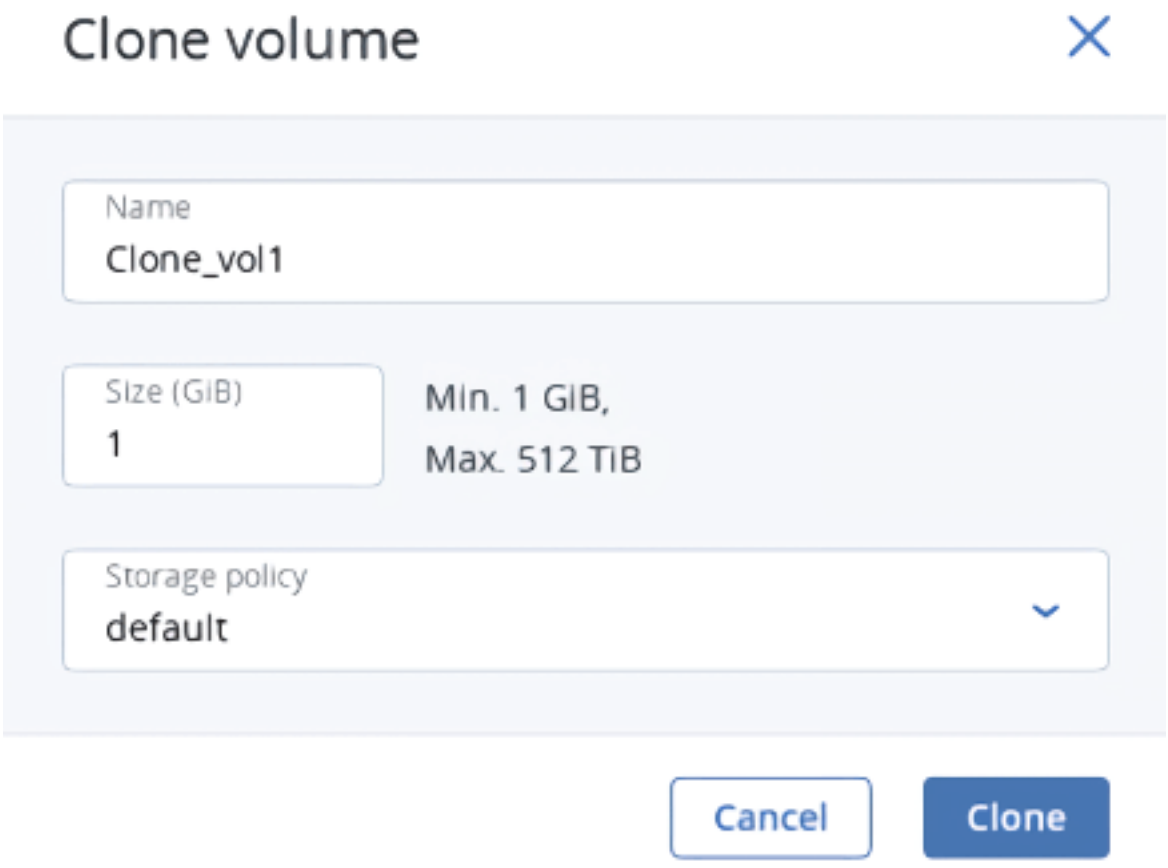
- Можно клонировать тома, которые не присоединены к ВМ или присоединены к остановленным ВМ.

Предварительные требования

- Создан том, как описано в разделе "Создание и удаление томов" (стр. 63).

Как клонировать том

1. На экране **Тома** щелкните по тому.
2. На правой панели тома нажмите **Клонировать**.
3. В окне **Клонировать том** укажите имя тома, размер и политику хранилища. Нажмите **Клонировать**.



5.5.7 Управление моментальными снимками томов

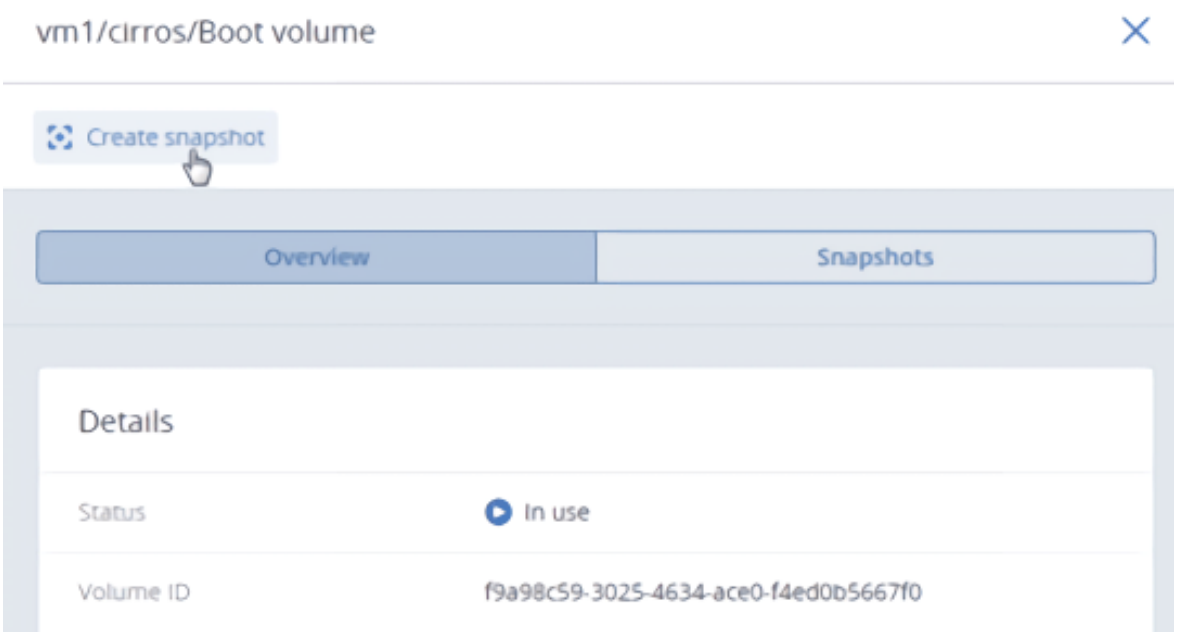
Можно сохранить текущее состояние файловой системы ВМ или пользовательских данных, создав моментальный снимок тома. Создание снимка загрузочного тома может оказаться полезным, например, перед обновлением ПО виртуальной машины. Если что-то пойдет не так, можно будет в любой момент вернуть ВМ в рабочее состояние. Снимок тома данных можно использовать для резервного копирования пользовательских данных или для тестирования.

Предварительные требования

- Чтобы создать согласованный снимок тома работающей ВМ, необходимо, чтобы в ВМ были установлены дополнения гостевой ОС, как описано в разделе "Установка дополнений гостевой ОС" (стр. 36). Гостевой агент QEMU, который входит в образ дополнений гостевой ОС, автоматически замораживает файловую систему во время создания снимка.

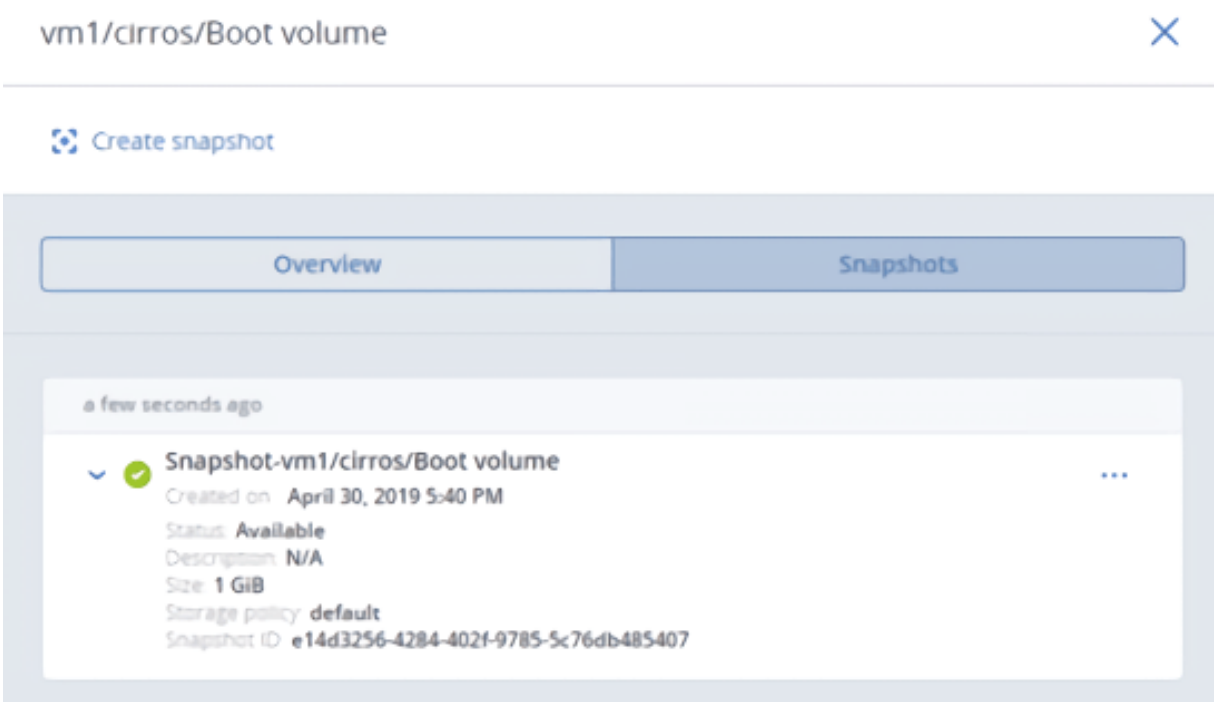
Как создать моментальный снимок тома

1. На экране **Тома** щелкните по тому.
2. На правой панели тома перейдите на вкладку **Снимки** и нажмите **Создать снимок**.



Как управлять моментальным снимком тома

Выберите том и откройте вкладку **Снимки** на его правой панели.



Можно выполнить следующие действия.

- Создать новый том из моментального снимка.
- Создать шаблон из моментального снимка.
- Отменить все изменения, внесенные в том с момента создания снимка. Это действие доступно только для виртуальных машин со статусами «Выключена» или «Ресурсы высвобождены».

  Предупреждение
  Поскольку для каждого тома существует только одна ветвь снимков, то все снимки, созданные после того снимка, к которому вы возвращаете состояние тома, будут удалены. Если вы хотите сохранить какой-либо последующий снимок перед возвратом, сначала создайте из него том или образ.

- Изменить имя или описание моментального снимка.
- Сбросить снимок, зависший в состоянии «Ошибка» или в переходном состоянии, в состояние «Доступно».
- Удалить моментальный снимок.

Чтобы выполнить эти действия, нажмите кнопку с многоточием рядом с моментальным снимком и выберите нужное действие.

5.6 Управление виртуальными сетями

Ограничения

- Вычислительную сеть можно удалить, только если к ней не подключены ВМ.

Как добавить новую виртуальную сеть

1. На странице **Сети** нажмите **Создать виртуальную сеть**.
2. На шаге **Конфигурация сети** выполните следующие действия.
   a. Включите или отключите управление IP-адресами:
      - Если управление IP-адресами включено, встроенный DHCP-сервер автоматически назначит ВМ, подключенным к сети, IP-адреса из пулов IP-адресов, а также задаст для ВМ настраиваемые DNS-серверы. Кроме того, по умолчанию для всех сетевых портов ВМ будет включена защита от спуфинга. Каждый сетевой интерфейс ВМ сможет принимать и отправлять IP-пакеты, только если ему назначены IP- и MAC-адреса. При необходимости защиту от спуфинга для интерфейса ВМ можно отключить вручную.
      - Если управление IP-адресами отключено, то ВМ, подключенные к сети, получат IP-адреса от DHCP-серверов в этой сети (при их наличии). Кроме того, защита от спуфинга будет отключена для всех сетевых портов ВМ, и ее нельзя будет включить вручную. Это означает, что каждый сетевой интерфейс ВМ с назначенными IP- и MAC-адресами или без них сможет принимать и отправлять IP-пакеты.

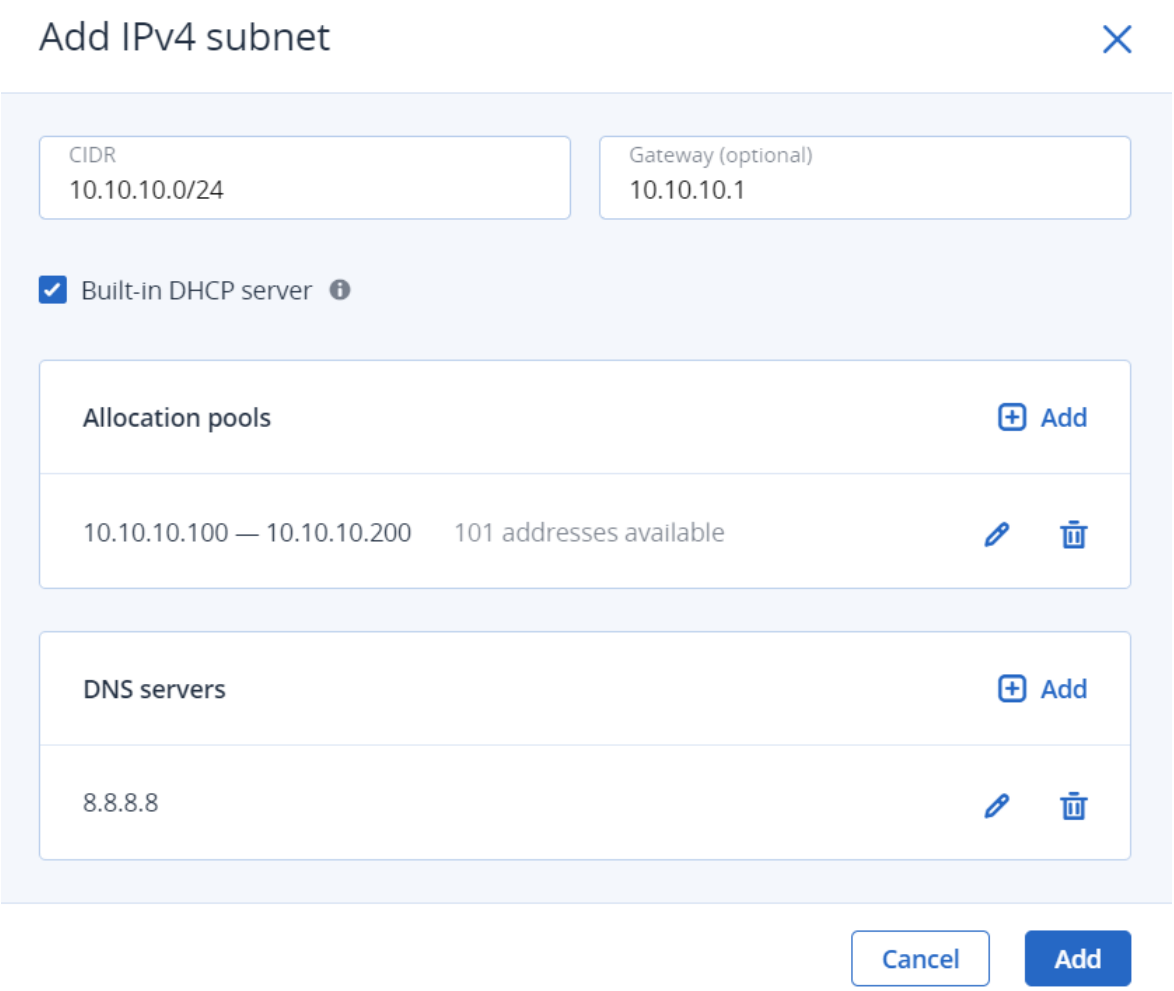
      В любом случае можно будет вручную назначить статические IP-адреса изнутри виртуальных машин.
   b. Укажите имя и нажмите **Далее**.

      Нет необходимости управлять несколькими системами передачи файлов.
3. Если вы включили управление IP-адресами, вы будете перенаправлены на шаг **Управление IP-адресами**, где можно добавить подсеть IPv4.
   a. В разделе **Подсети** нажмите **Добавить** и выберите **Подсеть IPv4**.
   b. В окне **Добавить подсеть IPv4** укажите диапазон адресов IPv4 сети, также при необходимости можно указать шлюз. Если оставить поле **Шлюз** пустым, то шлюз будет исключен из сетевых параметров.
   c. Включите или отключите встроенный DHCP-сервер:
      - Если DHCP-сервер включен, сетевым интерфейсам ВМ будут автоматически назначены IP-адреса: либо из пулов IP-адресов, либо при отсутствии пулов из всего диапазона IP-адресов сети. DHCP-сервер получит первые два IP-адреса из пула IP-адресов. Например:
        - В подсети 192.168.128.0/24 без шлюза DHCP-серверу будут назначены IP-адреса 192.168.128.1 и 192.168.128.2.
        - В подсети 192.168.128.0/24, в которой шлюзу назначен IP-адрес 192.168.128.1, DHCP-серверу будут назначены IP-адреса 192.168.128.2 и 192.168.128.3.
      - Если DHCP-сервер отключен, сетевые интерфейсы ВМ все равно получат IP-адреса, но их нужно будет назначить вручную внутри виртуальных машин.

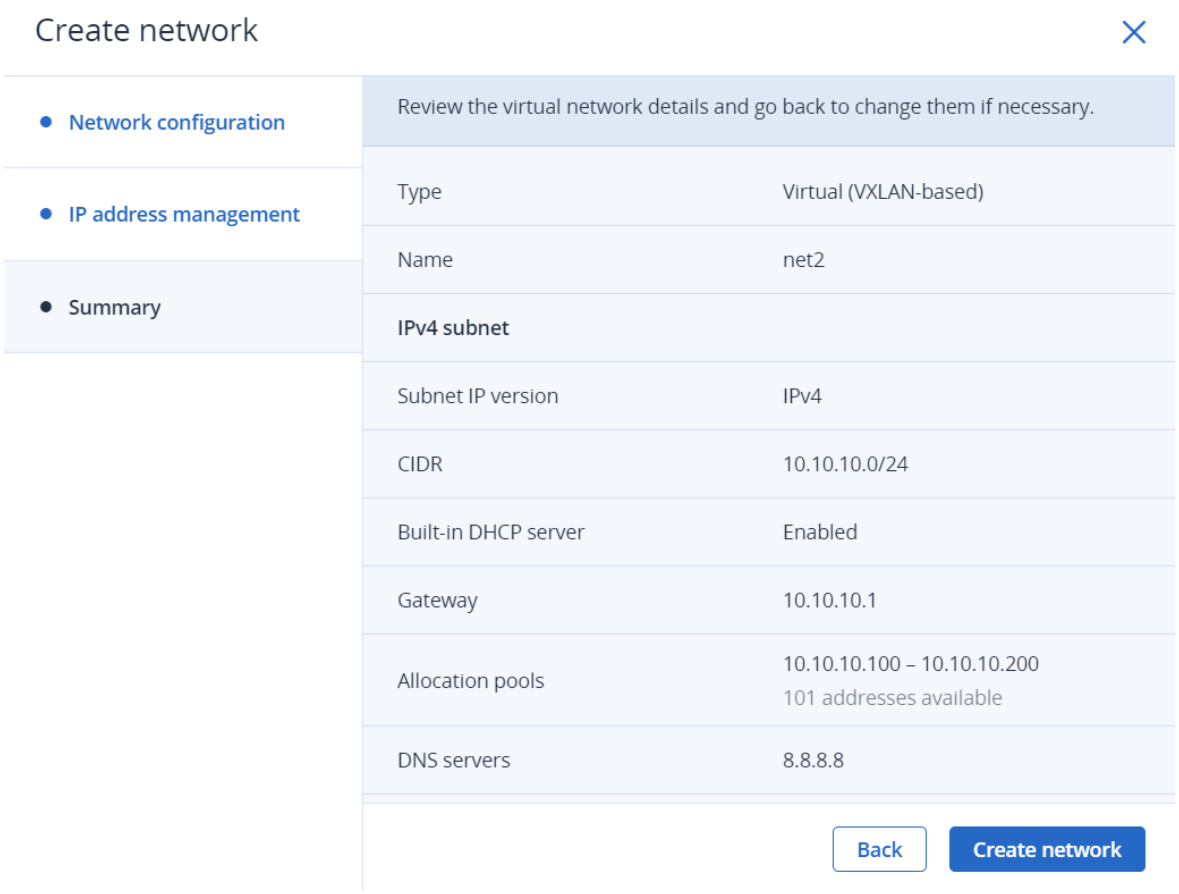
      Виртуальный DHCP-сервер будет работать только внутри текущей сети и не будет виден из других сетей.
   d. Укажите один или несколько пулов IP-адресов (диапазоны IP-адресов, которые будут автоматически назначаться виртуальным машинам).

e. Укажите DNS-серверы, которые будут использоваться виртуальными машинами. Эти серверы могут предоставляться виртуальным машинам посредством встроенного DHCP-сервера либо с помощью сетевой конфигурации cloud-init (если пакет cloud-init установлен в ВМ).

f. Нажмите **Добавить**.



4. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать виртуальную сеть**.



Как изменить параметры виртуальной сети

1. На экране **Сети** щелкните по нужной сети.
2. На правой панели сети нажмите значок карандаша рядом с именем сети или подсетью IPv4.
3. Внесите изменения и сохраните их.

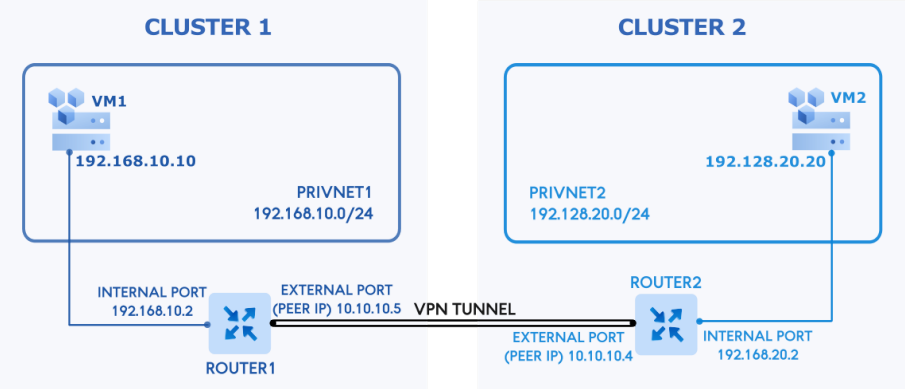
Как удалить вычислительную сеть

Нажмите значок с многоточием рядом с нужной сетью и выберите **Удалить**. Для одновременного удаления нескольких вычислительных сетей выделите их все и нажмите **Удалить**.

5.7 Управление соединениями VPN

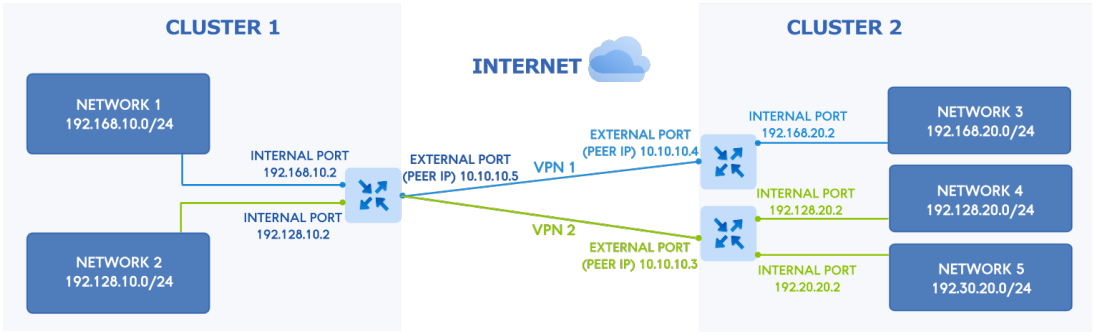
Виртуальная частная сеть как услуга (VPN as a Service) – это возможность, предоставляемая продуктом Кибер Инфраструктура, с помощью которой пользователи самообслуживания могут соединять виртуальные сети через общедоступные сети, такие как Интернет. Для соединения двух или более конечных точек виртуальные частные сети используют виртуальные соединения, для которых выполнятся туннелирование через физические сети. Для обеспечения безопасности обмена данными при использовании VPN трафик, проходящий между удаленными конечными точками, шифруется. Реализация VPN в продукте Кибер Инфраструктура использует протоколы Internet Key Exchange (IKE) и IP Security (IPsec), чтобы устанавливать безопасные соединения VPN, и основана на IPsec-решении strongSwan.

Чтобы лучше понять, как работает VPN, рассмотрим следующий пример:



- В кластере **cluster 1** виртуальная машина **VM1** подключена к виртуальной сети **privnet1** (192.168.10.0/24) через сетевой интерфейс с IP-адресом 192.168.10.10. Сеть **privnet1** открыта для доступа через общедоступные сети через маршрутизатор **router1** с внешним портом 10.10.10.5.
- В кластере **cluster 2** виртуальная машина **VM2** подключена к виртуальной сети **privnet2** (192.168.20.0/24) через сетевой интерфейс с IP-адресом 192.168.20.20. Сеть **privnet2** открыта для доступа через общедоступные сети через маршрутизатор **router2** с внешним портом 10.10.10.4.
- Туннель VPN создан между маршрутизаторами **router1** и **router2**, которые служат в качестве шлюзов VPN, таким образом обеспечивая взаимную связь между сетями **privnet1** и **privnet2**.
- Виртуальные машины **VM1** и **VM2** доступны друг для друга по их частным IP-адресам. То есть, **VM1** имеет доступ к **VM2** по IP-адресу 192.168.20.20, а **VM2** имеет доступ к **VM1** по IP-адресу 192.168.10.10.

Для обмена ключами между сторонами соединения доступны две версии IKE: IKE версия 1 (IKEv1) и IKE версия 2 (IKEv2). IKEv2 является самой последней версией протокола IKE и поддерживает возможность соединения нескольких удаленных подсетей.



В примере выше:

- **VPN1** использует IKEv1 и соединяет сеть **network1** с сетью **network3**.
- **VPN2** использует IKEv2 и соединяет сеть **network2** с сетями **network4** и **network5**.

5.7.1 Создание соединений VPN

Ограничения

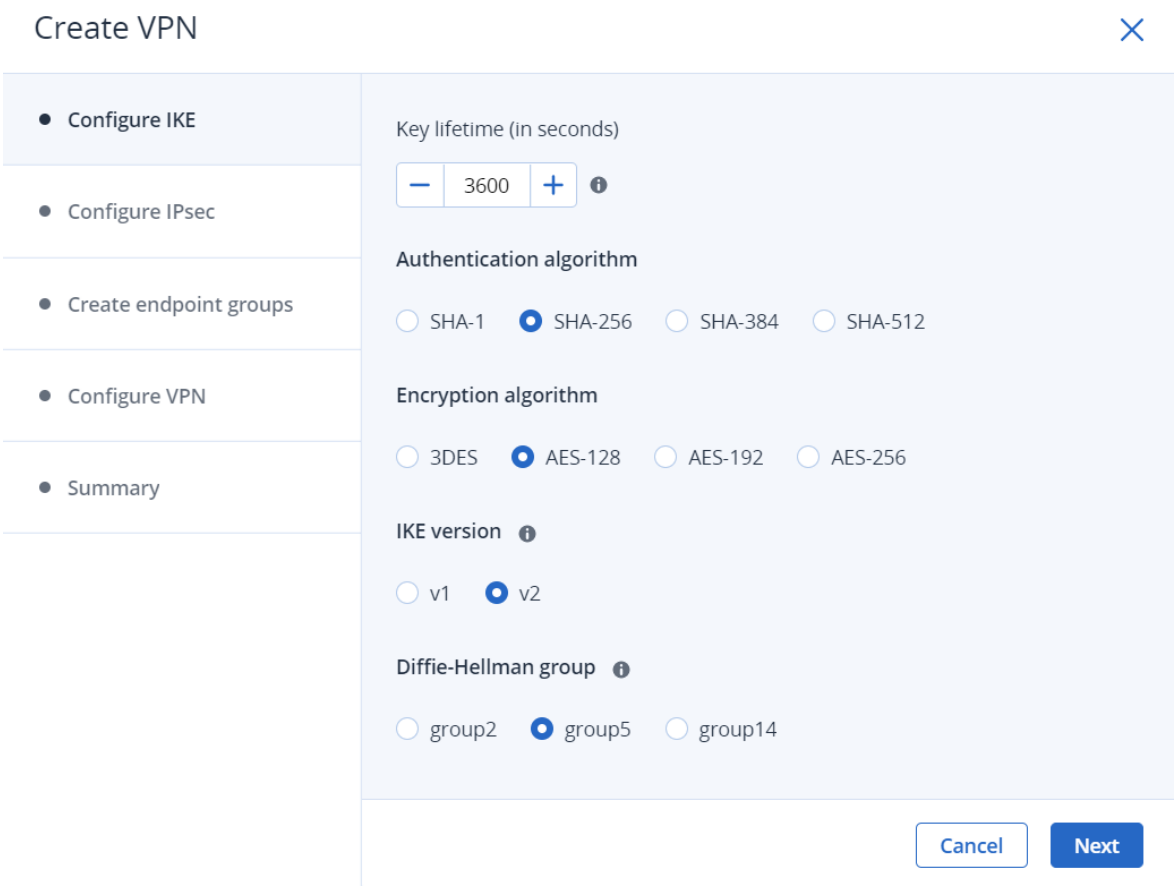
- У виртуальной машины не должно быть плавающих IP-адресов, назначенных ее частному сетевому интерфейсу. В противном случае трафик виртуальной машины не сможет быть направлен через туннель VPN.

Предварительные требования

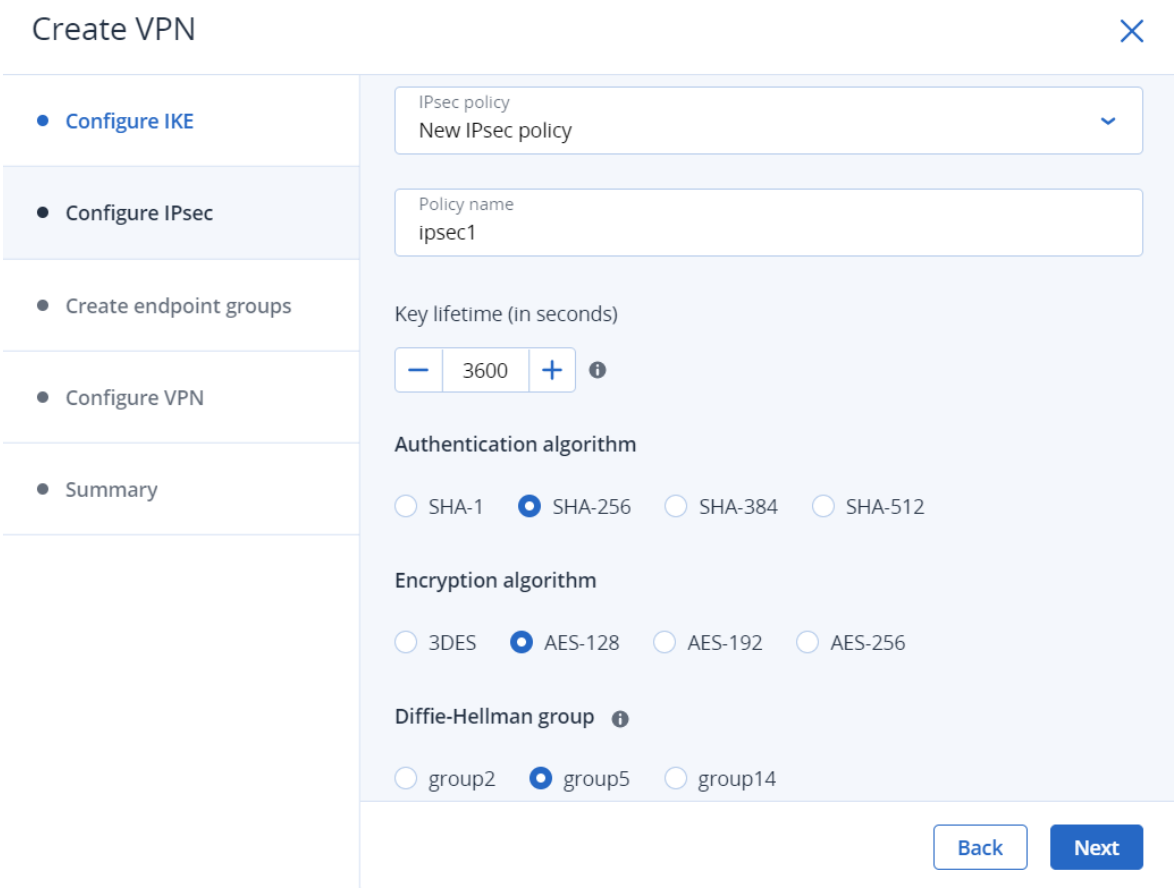
- Создан виртуальный маршрутизатор, как описано в разделе "Управление виртуальными маршрутизаторами" (стр. 79).
- Виртуальный маршрутизатор соединяет физическую сеть и виртуальные сети, доступ к которым необходимо предоставить через соединение VPN.
- Диапазоны IP-адресов сетей, которые будут соединены через туннель VPN, не должны перекрываться.

Чтобы создать соединение VPN

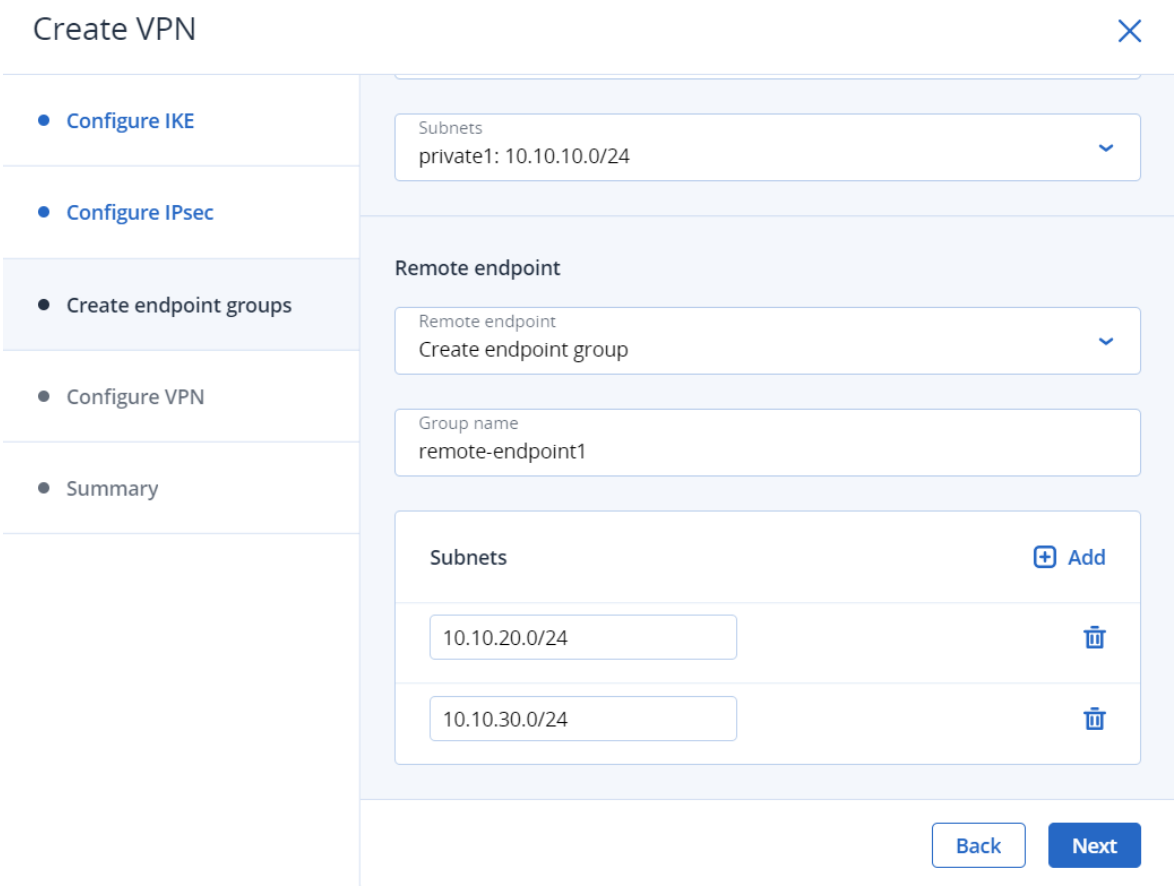
1. На экране **VPN** нажмите **Создать VPN**.
2. На шаге **Настроить IKE** укажите параметры политики IKE, которые будут использоваться для установки соединения VPN. Можно выбрать существующую политику IKE или создать новую. Для новой политики IKE сделайте следующее:
   a. Укажите пользовательское имя политики IKE.
   b. Укажите срок действия ключа в секундах, чтобы задать интервал обновления ключей. Срок действия ключа IKE должен быть больше, чем срок действия ключа IPsec.
   c. Выберите алгоритм аутентификации, который будет использоваться для проверки целостности и подлинности данных.
   d. Выберите алгоритм шифрования, который будет использоваться для обеспечения невозможности просмотра данных при транспортировке.
   e. Выберите версию IKE (1 или 2). Версия 1 обладает ограничениями, например, в ней нет поддержки возможности соединения нескольких подсетей.
   f. Выберите группу Диффи – Хеллмана, которая будет использоваться для создания ключа шифрования для процесса обмена ключами. Чем больше номер группы, тем более высокий уровень безопасности будет обеспечиваться, однако вычисление ключа будет занимать больше времени.
   g. Нажмите **Далее**.



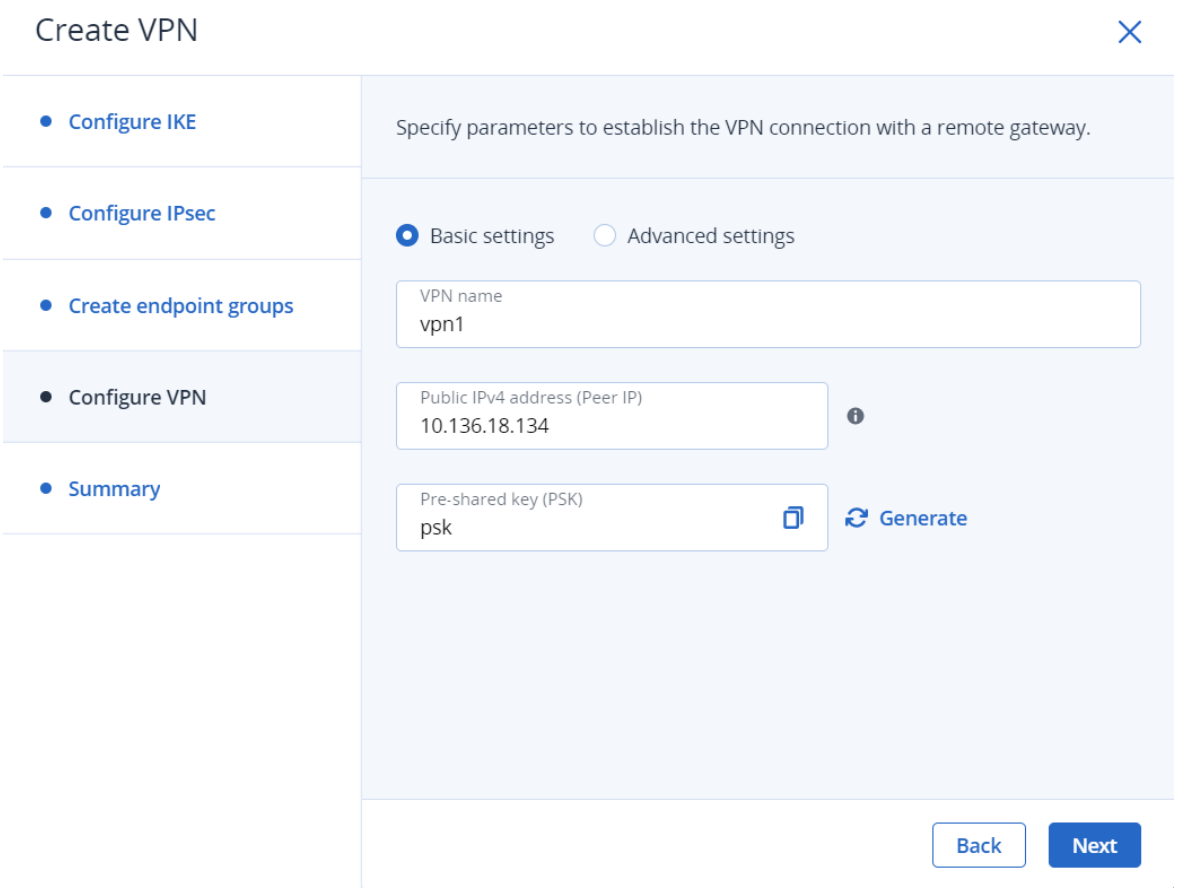
3. На шаге **Настроить IPsec** укажите параметры политики IPsec, которая будет использоваться для шифрования трафика VPN. Можно выбрать существующую политику IPsec или создать новую. Для новой политики IPsec сделайте следующее:
   a. Укажите пользовательское имя политики IPsec.
   b. Укажите срок действия ключа в секундах, чтобы задать интервал обновления ключей. Срок действия ключа IPsec не должен превышать срок действия ключа IKE.
   c. Выберите алгоритм аутентификации, который будет использоваться для проверки целостности и подлинности данных.
   d. Выберите алгоритм шифрования, который будет использоваться для обеспечения невозможности просмотра данных при транспортировке.
   e. Выберите группу Диффи – Хеллмана, которая будет использоваться для создания ключа шифрования для процесса обмена ключами. Чем больше номер у группы, тем более высокий уровень безопасности будет обеспечиваться, однако вычисление ключа будет занимать больше времени.
   f. Нажмите **Далее**.



4. На шаге **Создать группы конечных точек** выберите виртуальный маршрутизатор и укажите локальные и удаленные подсети, которые будут соединены через туннель VPN. Можно выбрать существующие локальные и удаленные конечные точки или создать новые. Для новых конечных точек сделайте следующее:
   a. Укажите пользовательское имя локальной конечной точки, а затем выберите локальные подсети.
   b. Укажите пользовательское имя удаленной конечной точки, а затем добавьте удаленные подсети. При добавлении подсетей используйте формат CIDR.
   c. Нажмите **Далее**.



5. На шаге **Настроить VPN** укажите параметры для установки соединения VPN с удаленным шлюзом:
   a. Укажите пользовательское имя соединения VPN.
   b. Укажите общедоступный адрес IPv4 удаленного шлюза, то есть IP-адрес стороны соединения VPN (peer IP address).
   c. Сгенерируйте предварительный общий ключ, который будет использоваться для аутентификации.
   d. [Необязательно] При необходимости можно также указать дополнительные параметры, выбрав **Расширенные настройки** и указав:
      - Идентификатор стороны соединения VPN (peer ID) для аутентификации и режим для установки соединения.
      - Политику Dead Peer Detection (DPD), а также интервал и время ожидания в секундах.
   e. Нажмите **Далее**.



6. На шаге **Сводка** просмотрите итоговую конфигурацию, а затем нажмите **Создать**.

Когда соединение VPN будет создано, его статус изменится с **Ожидание создания** на **Неактивно**. Соединение станет активным, как только туннель VPN будет настроен другой стороной соединения VPN и будет выполнена успешная авторизация IKE.

Внимание
Обе стороны соединения VPN должны использовать одну и ту же конфигурацию IKE и IPsec, в противном случае соединение VPN между ними не будет установлено.

5.7.2 Изменение конфигурации соединений VPN

После создания соединения VPN в любой момент времени можно изменить его группы конечных точек и параметры VPN.

Ограничения

- Нельзя менять виртуальный маршрутизатор и политики безопасности, которые используются для установки соединения VPN.

Предварительные требования

- Создано соединение VPN, как описано в разделе "Создание соединений VPN" (стр. 74).

Чтобы изменить конфигурацию соединения VPN

1. На экране **VPN** выберите необходимое соединение VPN.
2. На панели свойств соединения нажмите **Изменить**.
3. В окне **Изменить VPN** настройте при необходимости локальные и удаленные конечные точки, а затем нажмите **Далее**.
4. На следующем шаге измените параметры VPN, такие как имя соединения, IP-адрес стороны соединения VPN (peer IP address) и ключ PSK. При необходимости можно настроить дополнительные параметры, выбрав **Расширенные настройки** и изменив необходимые параметры.
5. Нажмите **Сохранить**, чтобы применить сделанные изменения.

После изменения параметров соединения его статус поменяется на **Неактивно**. Соединение будет повторно инициализировано, как только соответствующие параметры будут обновлены аналогичным образом другой стороной соединения VPN.

Внимание
Обе стороны соединения VPN должны использовать одну и ту же конфигурацию IKE и IPsec, в противном случае соединение VPN между ними не будет установлено.

5.7.3 Перезапуск и удаление соединений VPN

При перезапуске соединения VPN выполняется повторная принудительная инициализация этого соединения. При удалении соединения VPN удаляются политики IKE и IPsec, а также группы конечных точек, которые были созданы для этого соединения.

Предварительные требования

- Создано соединение VPN, как описано в разделе "Создание соединений VPN" (стр. 74).

Чтобы перезапустить соединение VPN

1. На экране **VPN** выберите необходимое соединение VPN.
2. На панели свойств соединения нажмите **Перезапустить**.
3. Нажмите **Перезапустить** в окне подтверждения.

Чтобы удалить соединение VPN

1. На экране **VPN** выберите необходимое соединение VPN.
2. На панели свойств соединения нажмите **Удалить**.
3. Нажмите **Удалить** в окне подтверждения.

5.8 Управление виртуальными маршрутизаторами

Виртуальные маршрутизаторы предоставляют сервисы L3, такие как маршрутизация и преобразование исходных сетевых адресов (SNAT), между виртуальными и физическими сетями либо различными виртуальными сетями.

- Виртуальный маршрутизатор между виртуальной и физической сетью обеспечивает доступ к внешним сетям, например к Интернету, для ВМ, подключенных к этой виртуальной сети.
- Виртуальный маршрутизатор между различными виртуальными сетями обеспечивает обмен данными по сети для ВМ, подключенных к этим виртуальным сетям.

У виртуального маршрутизатора есть два типа портов:

- Внешний шлюз, подключенный к физической сети.
- Внутренний порт, подключенный к виртуальной сети.

С виртуальными маршрутизаторами можно выполнить следующие действия.

- Создать виртуальные маршрутизаторы
- Изменить внешние или внутренние интерфейсы маршрутизатора
- Создать, изменить и удалить статические маршруты
- Изменить имя маршрутизатора
- Удалить маршрутизатор

Ограничения

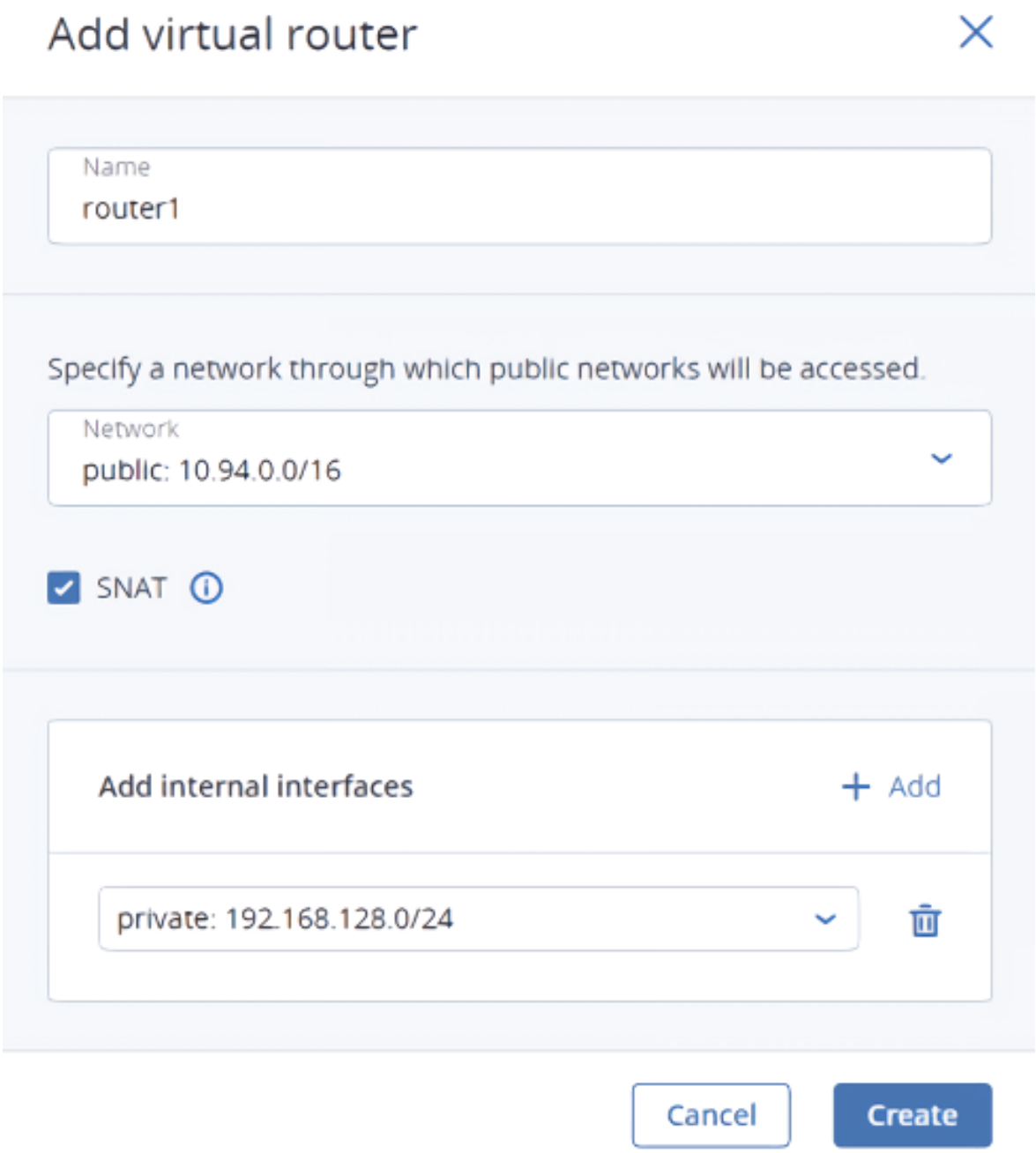
- Маршрутизатор может соединять только сети с включенным управлением IP-адресами.
- Виртуальный маршрутизатор можно удалить, если ни с одной из подключенных к нему сетей не связаны плавающие IP-адреса.

Предварительные требования

- Созданы вычислительные сети, как описано в разделе "Управление виртуальными сетями" (стр. 69).
- Для вычислительных сетей, которые будут подключены к маршрутизатору, указан шлюз.

Как создать виртуальный маршрутизатор

1. Перейдите на экран **Маршрутизаторы** и нажмите **Добавить маршрутизатор**.
2. В окне **Добавить маршрутизатор** выполните следующие действия.
   a. Укажите имя маршрутизатора.
   b. В раскрывающемся списке **Сеть** выберите физическую сеть, через которую будет предоставляться внешний доступ посредством внешнего шлюза. Новый внешний шлюз получит неиспользуемый IP-адрес из выбранной физической сети.
   c. В разделе **Добавить внутренние интерфейсы** выберите одну или несколько виртуальных сетей для подключения к маршрутизатору через внутренние интерфейсы. Новые внутренние интерфейсы по умолчанию будут пытаться использовать IP-адрес шлюза выбранных виртуальных сетей.
   d. [Необязательно] Установите или снимите флажок **SNAT**, чтобы включить или отключить SNAT на внешнем шлюзе маршрутизатора. При включенном преобразовании SNAT маршрутизатор заменяет частные IP-адреса ВМ публичным IP-адресом внешнего шлюза.



3. Нажмите кнопку **Создать**.

5.8.1 Управление интерфейсами маршрутизаторов

Предварительные требования

- Создан виртуальный маршрутизатор, как описано в разделе "Управление виртуальными маршрутизаторами" (стр. 79).

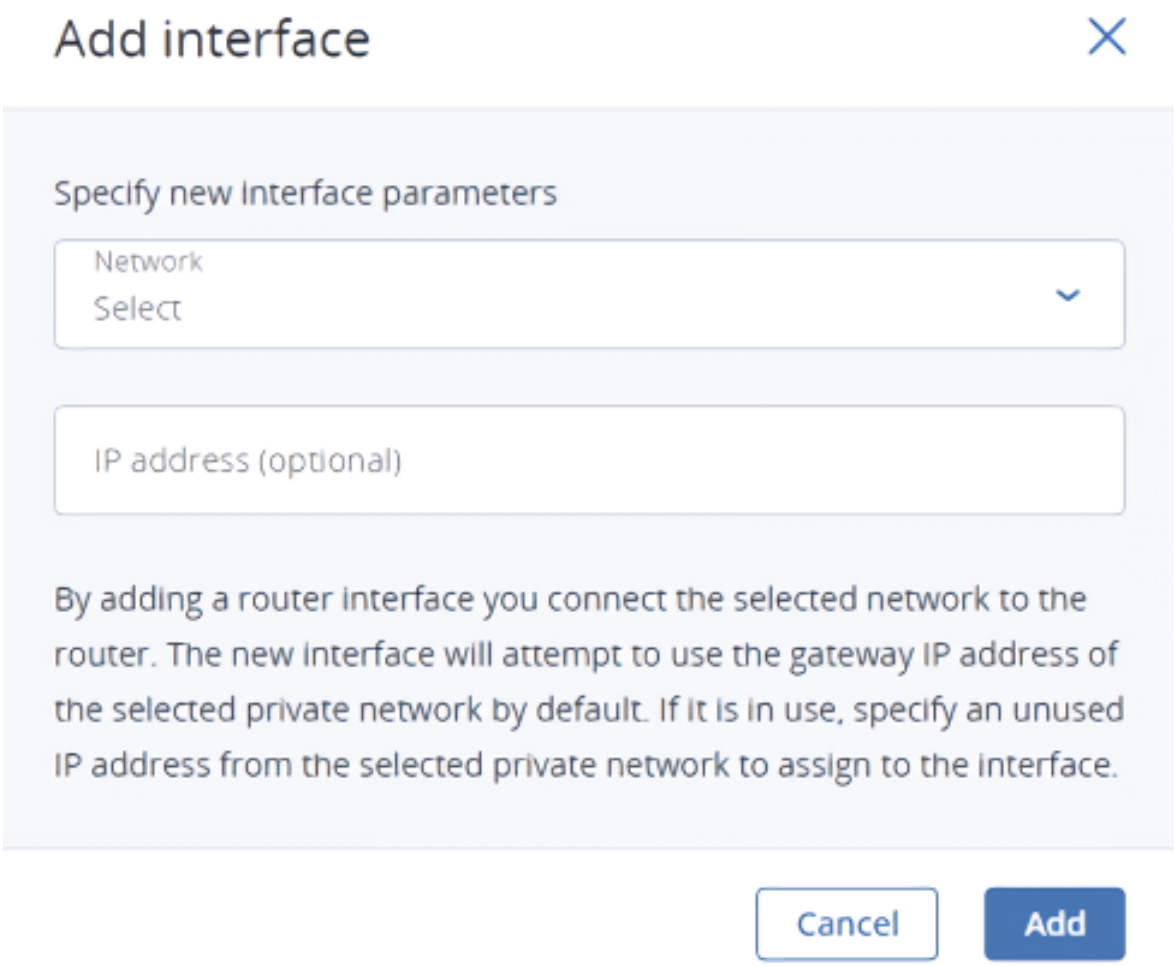
Как добавить внешний интерфейс маршрутизатора

1. Если у вас уже есть внешний шлюз, сначала удалите существующий.
2. На странице **Маршрутизаторы** нажмите имя маршрутизатора, чтобы открыть список его интерфейсов.
3. Нажмите **Добавить** на панели инструментов либо нажмите **Добавить интерфейс**, если не отображается ни одного интерфейса.
4. В окне **Добавить интерфейс** выполните следующие действия.
   a. Выберите **Внешний шлюз**.
   b. В раскрывающемся списке **Сеть** выберите физическую сеть для подключения к маршрутизатору. Новый интерфейс получит неиспользуемый IP-адрес из выбранной физической сети. Также можно указать определенный IP-адрес из выбранной сети и назначить его интерфейсу в поле **IP-адрес**.
   c. [Необязательно] Установите или снимите флажок **SNAT**, чтобы включить или отключить SNAT на внешнем шлюзе маршрутизатора. При включенном преобразовании SNAT маршрутизатор заменяет частные IP-адреса ВМ публичным IP-адресом внешнего шлюза.

5. Нажмите **Добавить**.

Как добавить внутренний интерфейс маршрутизатора

1. На странице **Маршрутизаторы** нажмите имя маршрутизатора, чтобы открыть список его интерфейсов.
2. Нажмите **Добавить**.
3. В окне **Добавить интерфейс** выберите сеть для подключения к маршрутизатору из раскрывающегося списка **Сеть**. Новый внутренний интерфейс по умолчанию будет пытаться использовать IP-адрес шлюза выбранной виртуальной сети. Если он уже используется, укажите неиспользуемый IP-адрес из выбранной виртуальной сети и назначьте его маршрутизатору в поле **IP-адрес**.



4. Нажмите **Добавить**.

Чтобы удалить интерфейс маршрутизатора, нажмите рядом с ним значок многоточия и выберите **Удалить**.

Как изменить параметры интерфейса маршрутизатора

1. Щелкните по значку многоточия рядом с интерфейсом и выберите **Изменить**.
2. В окне **Изменить интерфейс** измените IP-адрес.
3. Для внешнего интерфейса включите или отключите SNAT.
4. Нажмите **Сохранить**, чтобы сохранить изменения.

Как удалить интерфейс маршрутизатора

1. Выберите интерфейс, который следует удалить.
2. Щелкните рядом с ним по значку многоточия и выберите **Удалить**.

5.8.2 Управление статическими маршрутами

Также можно настроить статические маршруты, вручную добавив записи в таблицу маршрутизации. Это может пригодиться, например, если вам не нужно двустороннее соединение между двумя виртуальными сетями, а требуется только доступ к одной виртуальной сети из другой.

Рассмотрим следующий пример:

- Виртуальная машина **VM1** подключена к виртуальной сети **private1** (192.168.128.0/24) через сетевой интерфейс с IP-адресом 192.168.128.10.
- Виртуальная машина **VM2** подключена к виртуальной сети **private2** (192.168.30.0/24) через сетевой интерфейс с IP-адресом 192.168.30.10.
- Маршрутизатор **router1** соединяет сеть **private1** с физической сетью через внешний шлюз с IP-адресом 10.94.129.73.
- Маршрутизатор **router2** соединяет сеть **private2** с физической сетью через внешний шлюз с IP-адресом 10.94.129.74.

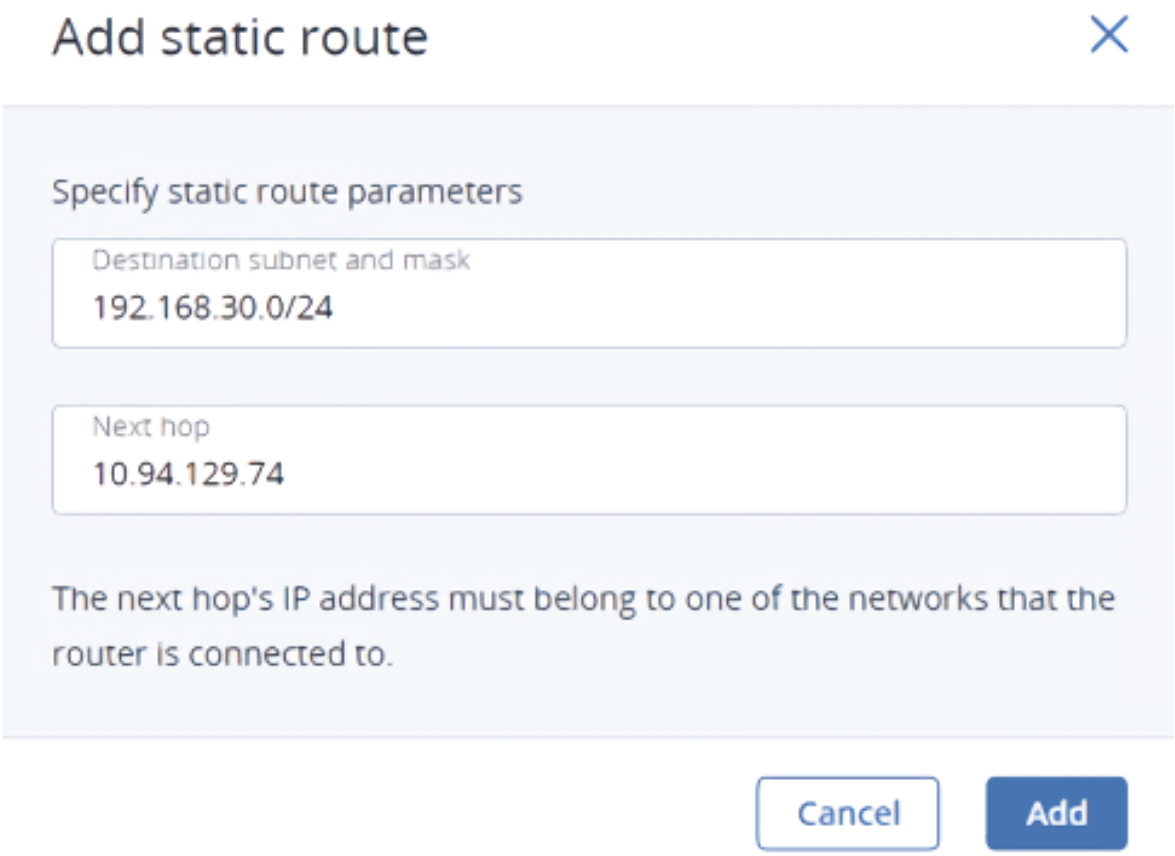
Для обеспечения доступа к **VM2** с **VM1** необходимо добавить статический маршрут для **router1**, указав CIDR сети **private2**, то есть 192.168.30.0/24, в качестве целевой подсети и IP-адрес внешнего шлюза **router2**, то есть 10.94.129.74, в качестве IP-адреса следующего транзитного участка. В этом случае, когда IP-пакет для 192.168.30.10 поступает на маршрутизатор **router1**, он перенаправляется на **router2**, а затем на **VM2**.

Предварительные требования

- Создан виртуальный маршрутизатор, как описано в разделе "Управление виртуальными маршрутизаторами" (стр. 79).

Как создать статический маршрут для маршрутизатора

1. На странице **Маршрутизаторы** щелкните по имени маршрутизатора. Откройте вкладку **Статические маршруты** и нажмите **Добавить** на панели справа. Если не отображается ни одного маршрута, нажмите **Добавить статический маршрут**.
2. В окне **Добавить статический маршрут** укажите диапазон и маску целевой подсети в нотации CIDR и IP-адрес следующего транзитного участка. IP-адрес следующего транзитного участка должен принадлежать одной из сетей, к которым подключен маршрутизатор.



3. Нажмите **Добавить**.

Как изменить статический маршрут

1. Щелкните по значку многоточия рядом с нужным статическим маршрутом и выберите **Изменить**.
2. В окне **Изменить статический маршрут** измените нужные параметры и нажмите **Сохранить**.

Как удалить статический маршрут

Щелкните по значку многоточия рядом со статическим маршрутом, который следует удалить, и выберите **Удалить**.

5.9 Управление плавающими IP-адресами

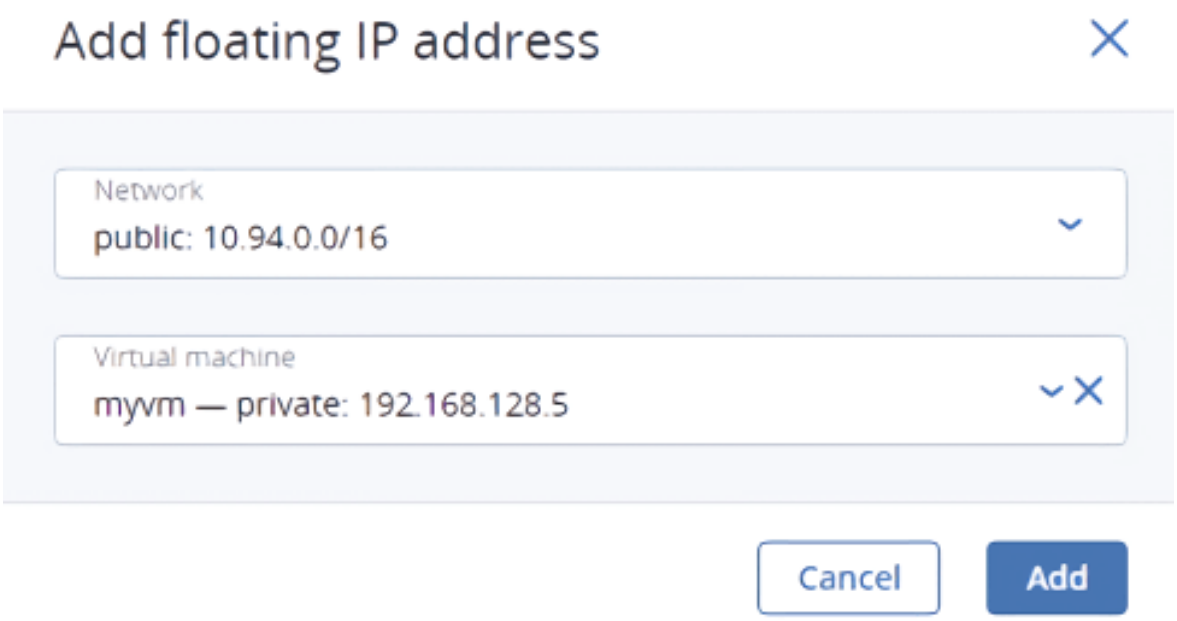
Виртуальная машина, подключенная к виртуальной сети, может быть доступна из внешних сетей, таких как Интернет, через плавающий IP-адрес. Такой адрес берется из физической сети и сопоставляется с частным IP-адресом ВМ. Плавающий и частный IP-адреса используются одновременно на сетевом интерфейсе ВМ. Частный IP-адрес предназначен для связи с другими ВМ в виртуальной сети. Плавающий IP-адрес предназначен для доступа к ВМ из внешних сетей. Гостевая операционная система ВМ не имеет сведений о назначенном плавающем IP-адресе.

Предварительные требования

- Создан виртуальный маршрутизатор, как описано в разделе "Управление виртуальными маршрутизаторами" (стр. 79).
- У виртуальной машины, которой следует назначить плавающий IP-адрес, есть фиксированный частный IP-адрес.
- Виртуальный маршрутизатор соединяет физическую сеть, из которой будет взят плавающий IP-адрес, с виртуальной сетью ВМ.

Как создать плавающий IP-адрес и назначить его виртуальной машине

1. На экране **Плавающие IP-адреса** нажмите **Добавить плавающий IP-адрес**.
2. В окне **Добавить плавающий IP-адрес** выберите физическую сеть, из которой будет взят плавающий IP, и сетевой интерфейс ВМ с фиксированным частным IP-адресом.



3. Нажмите **Добавить**.

Как переназначить плавающий IP-адрес другой виртуальной машине

1. Нажмите значок с многоточием напротив плавающего IP-адреса и выберите **Снять назначение**.
2. Когда имя ВМ исчезнет из столбца **Назначен**, снова нажмите значок с многоточием и выберите **Назначить**.
3. В окне **Назначить плавающий IP-адрес** выберите сетевой интерфейс ВМ с фиксированным частным IP-адресом.
4. Нажмите **Назначить**.

Как удалить плавающий IP-адрес

1. Отмените его назначение виртуальной машине. Нажмите значок с многоточием напротив плавающего IP-адреса и выберите **Снять назначение**.
2. Снова нажмите значок с многоточием и выберите **Удалить**.

5.10 Управление балансировщиками нагрузки

Кибер Инфраструктура предлагает балансировку нагрузки как сервис для вычислительной инфраструктуры. Балансировка нагрузки обеспечивает отказоустойчивость и повышает производительность веб-приложений путем распределения входящего сетевого трафика по виртуальным машинам из пула балансировки. Балансировщик нагрузки получает и перенаправляет входящие запросы на подходящую ВМ в зависимости от настроенного алгоритма балансировки и состояния ВМ.

Ограничения

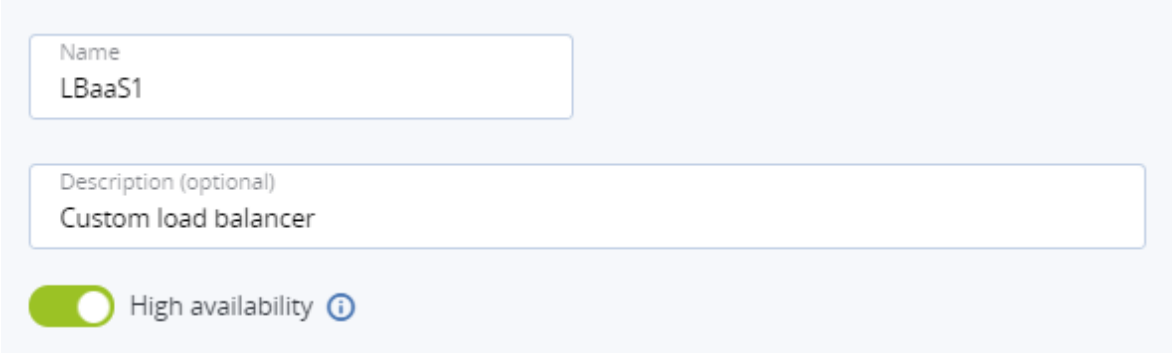
- Правило перенаправления и протокол нельзя будет изменить после создания балансировщика.

Предварительные требования

- Для сети, в которой будет работать балансировщик нагрузки, включено управление IP-адресами.
- У всех ВМ, которые будут добавлены в пулы балансировки, есть фиксированные IP-адреса.

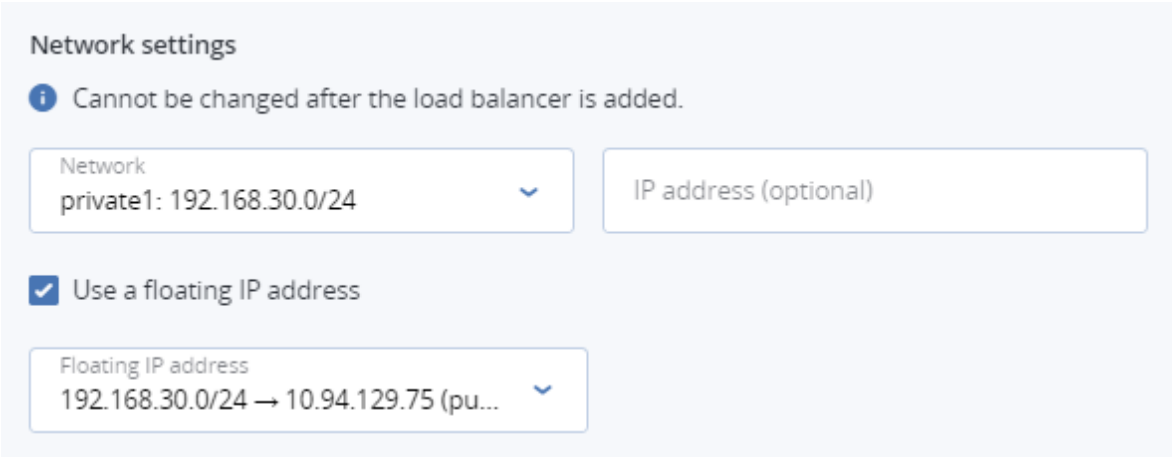
Как создать балансировщик нагрузки с пулами балансировки

1. На экране **Балансировщики нагрузки** нажмите **Создать балансировщик нагрузки**.
2. В окне **Создать балансировщик нагрузки** выполните следующие действия.
   a. Укажите имя и при необходимости описание.
   b. Включите или отключите высокую доступность.
      - При включенной высокой доступности будет создано два экземпляра балансировщика нагрузки. Они будут работать в режиме Active/Standby в соответствии с протоколом VRRP (Virtual Router Redundancy Protocol).
      - При отключенной высокой доступности будет создан один экземпляр балансировщика нагрузки.



3. В разделе **Сетевые параметры** выберите сеть, в которой будет работать балансировщик нагрузки, и по желанию укажите IP-адрес, который будет выделен балансировщику нагрузки.
4. Если выбранная виртуальная сеть подключена к физической сети через маршрутизатор, можно назначить балансировщику нагрузки плавающий IP-адрес. Для этого установите флажок **Использовать плавающий IP-адрес**. Появится раскрывающееся меню, в котором можно

выбрать, следует использовать доступный плавающий IP-адрес или создать новый.



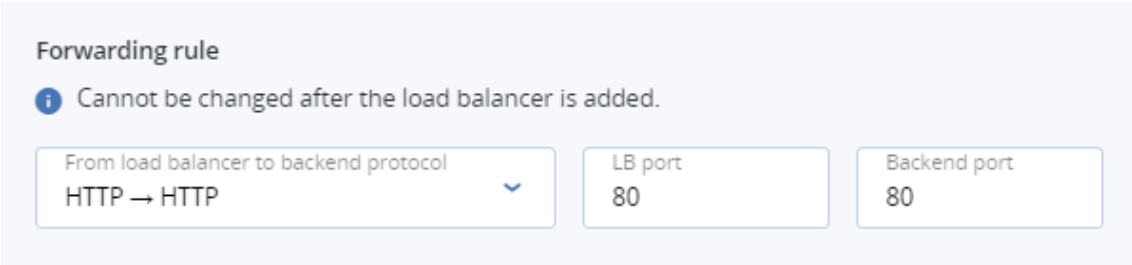
5. В разделе **Пулы балансировки** нажмите кнопку **Добавить**, чтобы создать пул балансировки для перенаправления трафика от балансировщика нагрузки на виртуальные машины.

   В открывшемся окне **Создать пул балансировки** выполните следующие действия.

   a. В разделе **Правило перенаправления** выберите правило перенаправления от балансировщика нагрузки на внутренний протокол, а затем укажите порты для входящих и целевых подключений.

      Обратите внимание на следующее.

      - С правилом **HTTPS -> HTTPS** все виртуальные машины должны иметь один SSL-сертификат (или цепочку сертификатов).
      - С правилом **HTTPS -> HTTP** необходимо загрузить SSL-сертификат (или цепочку сертификатов) в формате PEM и закрытый ключ в формате PEM.



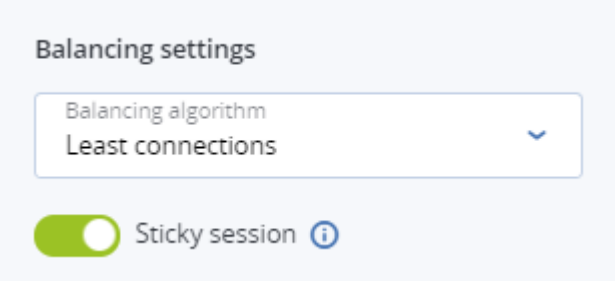
   b. В разделе **Параметры балансировки** выберите алгоритм балансировки.

      - **Least connections** (Минимум подключений). Запросы будут перенаправлены на ВМ с наименьшим количеством активных подключений.
      - **Round robin** (Круговое обслуживание). Все ВМ будут получать запросы методом циклического перебора.
      - **Source IP** (IP отправителя). Запросы от уникального IP-адреса отправителя будут направляться на одну и ту же ВМ.

      Включите/отключите параметр **Sticky session** (Закрепить сеанс), чтобы включить или отключить сохранение сеанса. Балансировщик нагрузки сформирует файл cookie, который будет вставляться в каждый ответ и применяться при отправке будущих запросов к той же ВМ.

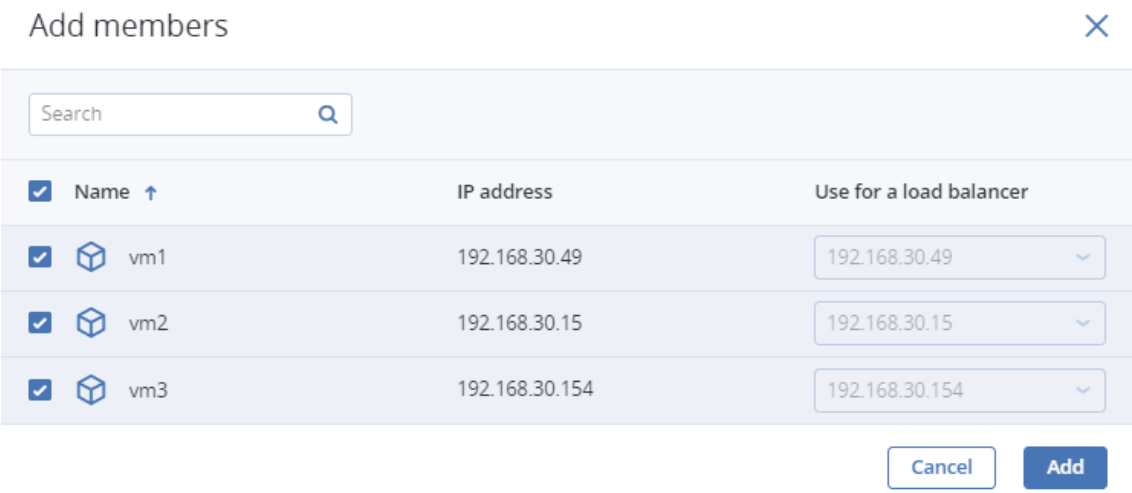
Примечание

Этот параметр недоступен в режиме сквозной передачи SSL Passthrough.



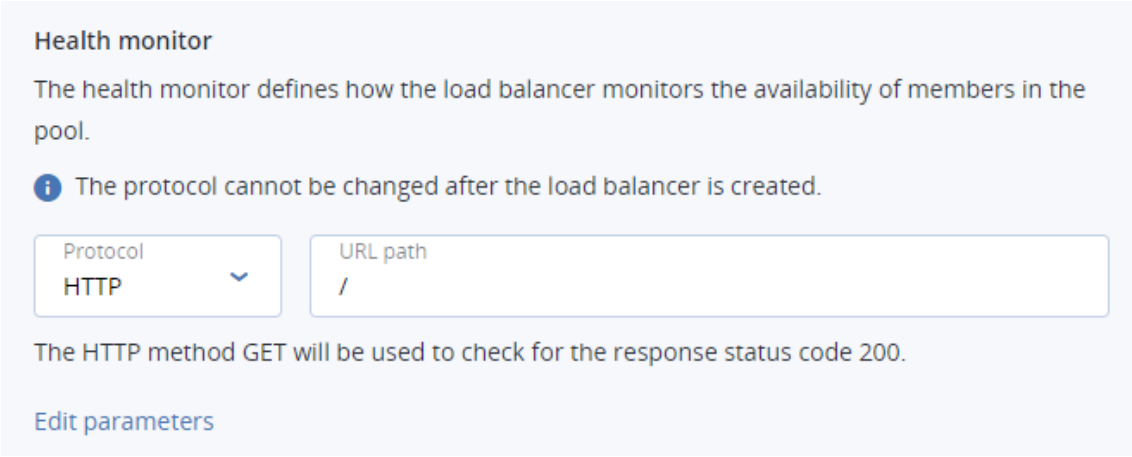
c. В разделе **Участники** нажмите кнопку **Добавить**, чтобы добавить участников, то есть виртуальные машины, в пул балансировки. Каждая ВМ может входить в несколько пулов балансировки.

В открывшемся окне **Добавить участников** выберите нужные ВМ и нажмите **Добавить**.

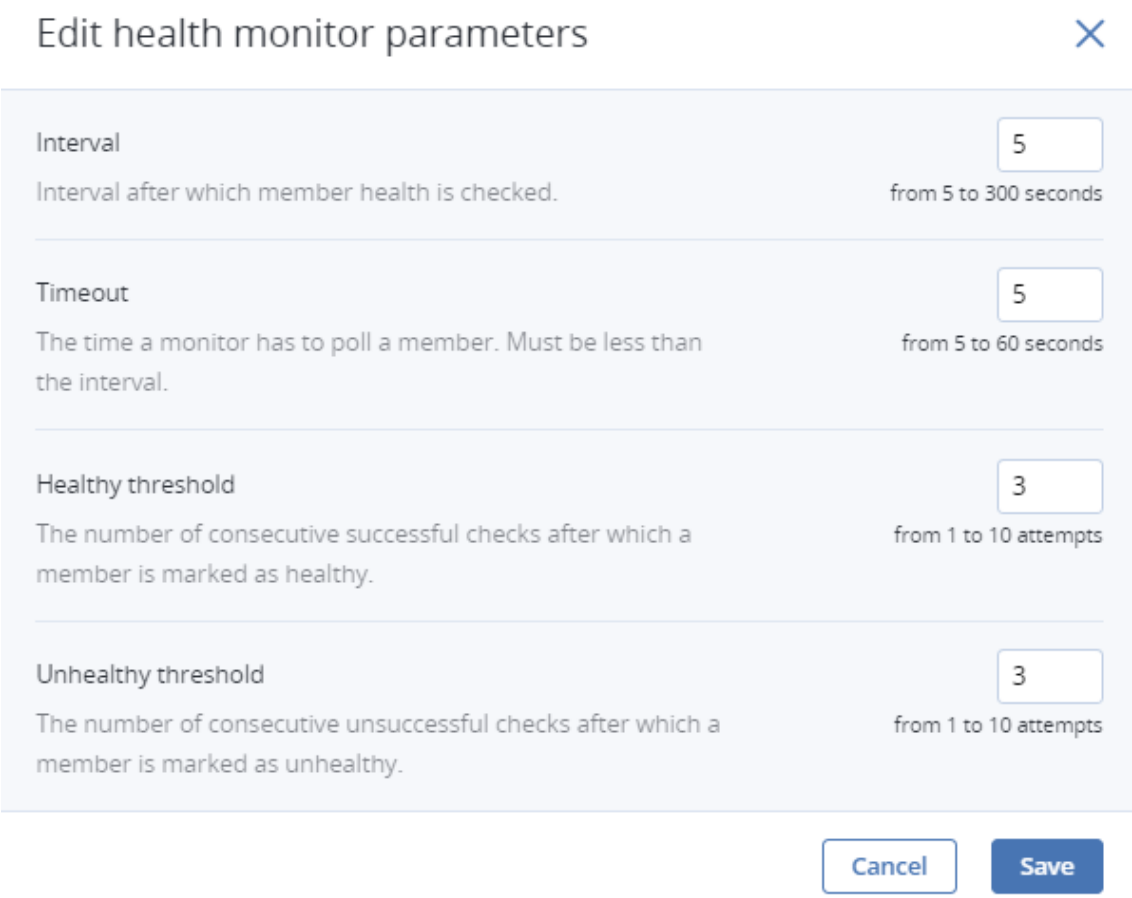


d. В разделе **Монитор состояния** выберите протокол, который будет использоваться для мониторинга доступности участников.

- **HTTP/HTTPS**. Для проверки ответного кода статуса 200 будет использоваться метод HTTP/HTTPS GET. Дополнительно укажите URL-путь к монитору состояния.
- **TCP/UDP**. Монитор состояния будет проверять TCP/UDP-подключение на внутреннем порте.
- **PING**. Монитор состояния будет проверять IP-адреса участников.

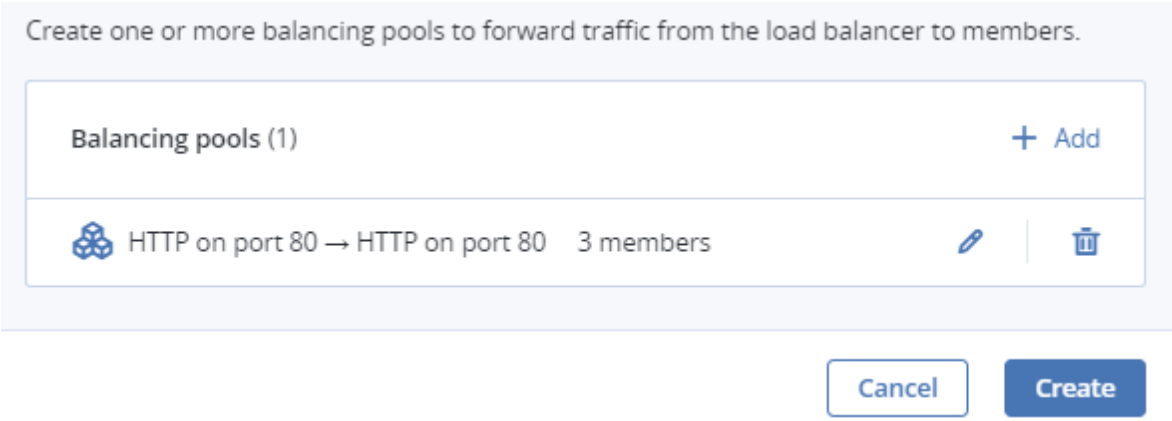


По умолчанию монитор состояния удаляет участника из пула балансировки, если три последовательные проверки состояния с интервалами в пять секунд заканчиваются неудачей. Когда участник возобновляет работу и успешно отвечает на три последовательные проверки, он снова добавляется в пул. Можно вручную задать параметры монитора состояния, такие как интервал проверки статуса ВМ, время ожидания монитора, пороговые значения исправности и неисправности. Чтобы изменить параметры по умолчанию, нажмите **Изменить параметры**, введите нужные значения и нажмите **Сохранить**.



e. Нажмите кнопку **Создать**.

6. [Необязательно] Добавьте другие пулы балансировки, как описано выше.
7. Нажмите кнопку **Создать**.



Как отслеживать производительность и состояние балансировщика нагрузки

Откройте вкладку **Сводка** на правой панели балансировщика нагрузки.

Доступны следующие диаграммы:

Состояние участников

Общее число участников в пулах балансировки, сгруппированных по статусу «Исправен», «Неисправен», «Ошибка» и «Отключен».

ЦП/ОЗУ

Использование ЦП и ОЗУ балансировщиком нагрузки.

Сеть

Входящий и исходящий сетевой трафик.

Активные подключения

Количество активных подключений.

Ошибочные запросы

Количество ошибочных запросов.

Как изменить имя или описание балансировщика нагрузки

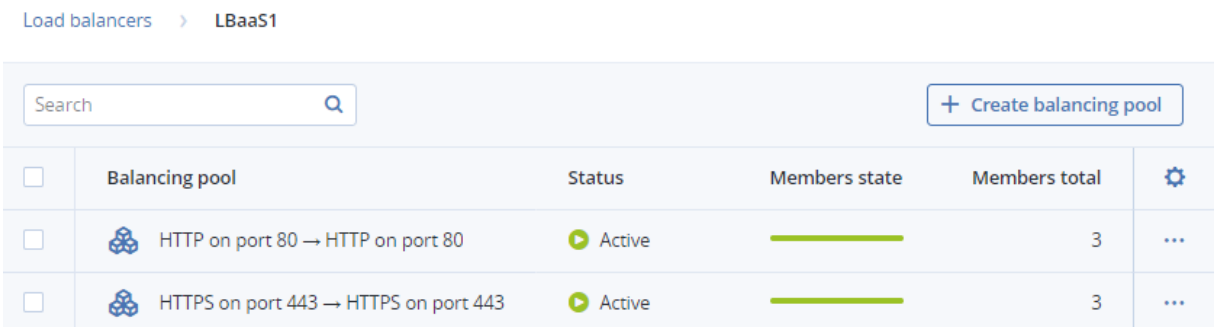
Щелкните по значку многоточия рядом с нужным балансировщиком нагрузки и выберите **Изменить**.

Как включить/отключить или удалить балансировщик нагрузки

Щелкните по значку многоточия рядом с балансировщиком нагрузки и выберите нужное действие. Для одновременного удаления нескольких балансировщиков нагрузки выделите их все и нажмите **Удалить**.

5.10.1 Управление пулами балансировки

Щелкните по имени балансировщика нагрузки, чтобы открыть список пулов балансировки.



Можно открыть правую панель пула, чтобы проверить его состояние и производительность на вкладке **Сводка**, просмотреть его параметры на вкладке **Свойства** и управлять его участниками на вкладке **Участники**.

Как добавить еще один пул в балансировщик нагрузки

Нажмите **Создать пул балансировки** и заполните поля, как описано в разделе "Управление балансировщиками нагрузки" (стр. 88). Добавленный пул появится в списке пулов балансировки.

Как изменить пул балансировки

- Чтобы изменить параметры балансировки, такие как алгоритм балансировки и сохранение сеансов, нажмите значок многоточия рядом с пулом и выберите **Изменить**.
- Чтобы изменить параметры монитора состояния, нажмите значок многоточия рядом с пулом и выберите **Изменить монитор состояния**.

Как добавить других участников в пул балансировки

Щелкните по значку многоточия рядом с нужным пулом балансировки и выберите **+ Добавить участников**.

Как удалить пул балансировки

Нажмите значок с многоточием рядом с нужным пулом балансировки и выберите **Удалить**. Для одновременного удаления нескольких пулов балансировки выделите их все и нажмите **Удалить**.

5.11 Управление SSH-ключами

SSH-ключи применяются для защищенного SSH-доступа к виртуальным машинам. Можно создать пару ключей на клиенте, с которого вы будете подключаться к виртуальным машинам через SSH. Закрытый ключ будет храниться на клиенте, и его можно будет скопировать на другие серверы. Открытый ключ необходимо будет загрузить в продукт Кибер Инфраструктура и указать при создании ВМ. Он внедряется в виртуальную машину посредством cloud-init и используется для аутентификации OpenSSH. Внедрение ключей поддерживается для виртуальных машин под управлением как Linux, так и Windows.

Ограничения

- SSH-ключ можно указать, только если ВМ развертывается из шаблона или загрузочного тома (не ISO-образа).

- Если ключ внедрен в одну или несколько ВМ, он останется в них даже после его удаления из панели.

Предварительные требования

- Утилита cloud-init и OpenSSH Server установлены на загрузочный том или в шаблон ВМ, как указано в разделе "Подготовка шаблонов" (стр. 57).

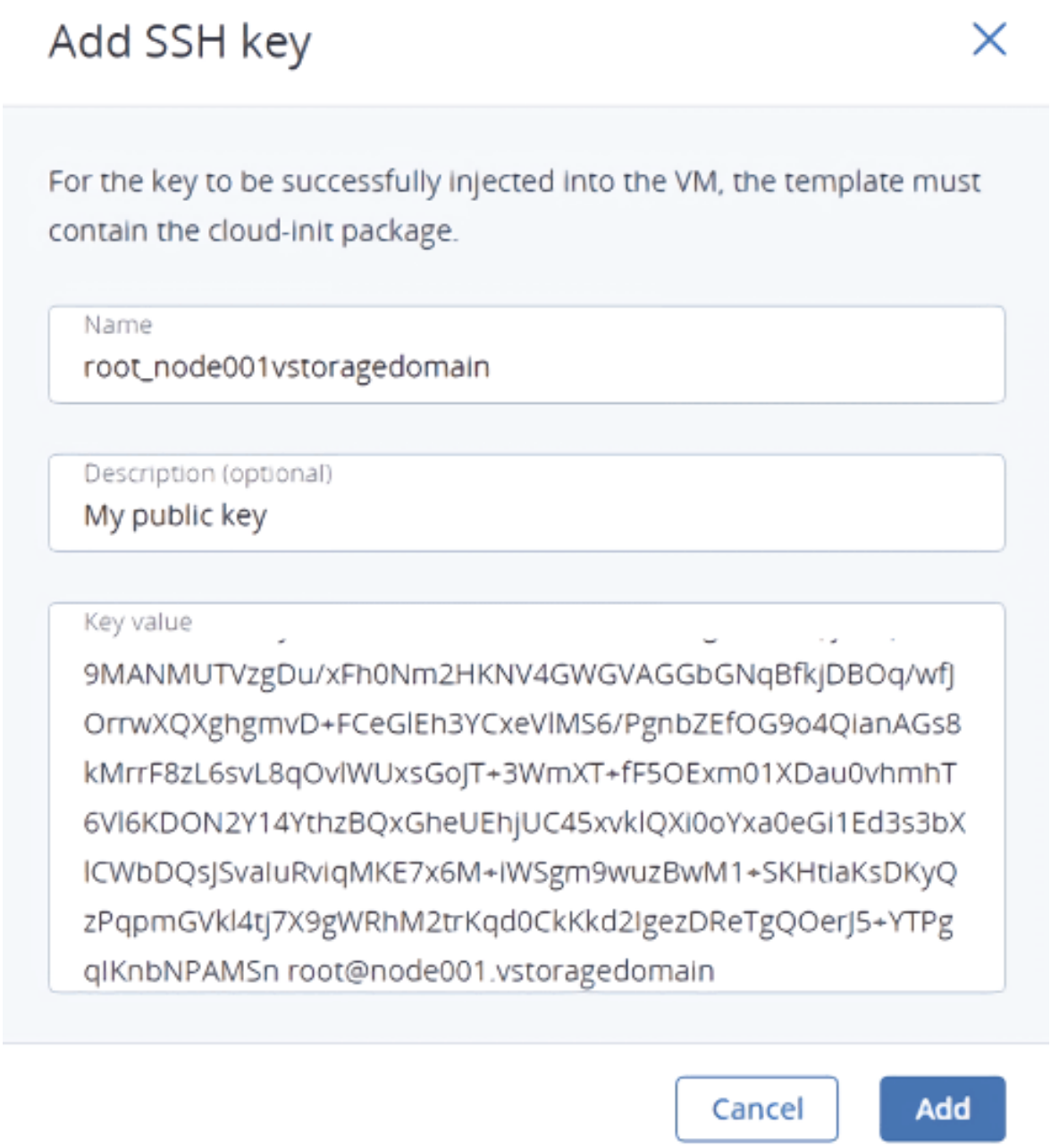
Как добавить открытый ключ

1. Создайте пару SSH-ключей на клиенте с помощью утилиты ssh-keygen.

   ```
   # ssh-keygen -t rsa
   ```

2. На экране **SSH-ключи** нажмите **Добавить ключ**.
3. В окне **Добавить SSH-ключ** укажите имя ключа и скопируйте значение из созданного открытого ключа, который находится в /root/.ssh/id_rsa.pub. При необходимости можно

добавить описание ключа.



Как удалить открытый ключ

1. На экране **SSH-ключи** выберите SSH-ключ, который следует удалить, и нажмите **Удалить**.
2. В окне подтверждения нажмите **Удалить**.

Если SSH-ключ был внедрен в какие-либо виртуальные машины, он останется внутри них.