

КИБЕРПРОТЕКТ



КИБЕР Инфраструктура

Версия 6.5

Заявление об авторских правах

Все права защищены.

Все остальные упоминаемые товарные знаки могут быть зарегистрированными товарными знаками соответствующих владельцев.

Распространение существенно измененных версий данного руководства запрещено без явного разрешения владельца авторских прав.

Распространение настоящих или переработанных материалов, входящих в данное руководство, в виде печатного издания (книги) запрещено без письменного разрешения их владельца.

ДОКУМЕНТАЦИЯ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». НЕ СУЩЕСТВУЕТ НИКАКИХ ЯВНО ВЫРАЖЕННЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ОБЯЗАТЕЛЬСТВ, ПОДТВЕРЖДЕНИЙ ИЛИ ГАРАНТИЙ, В ТОМ ЧИСЛЕ И СВЯЗАННЫХ С ТОВАРНОСТЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ ПРИГОДНОСТЬЮ ЕГО ДЛЯ ИСПОЛЬЗОВАНИЯ В ОПРЕДЕЛЕННЫХ ЦЕЛЯХ, НАСКОЛЬКО ТАКАЯ ОГРАНИЧЕННОСТЬ ОТВЕТСТВЕННОСТИ ДОПУСКАЕТСЯ ЗАКОНОМ.

С ПО или Услугой может быть предоставлен исходный код сторонних производителей. Лицензии этих сторонних производителей подробно описаны в файле `license.txt`, находящемся в корневом каталоге установки.

Содержание

1 Введение	4
2 Аппаратные требования	5
3 Установка Кибер Инфраструктура	6
4 Создание кластера хранилища данных	8
5 Включение высокой доступности сервера управления	9
6 Развертывание вычислительного кластера	11
7 Создание виртуальной машины	19

1 Введение

Кибер Инфраструктура представляет собой новое поколение гиперконвергентных инфраструктур, предназначенных как для поставщиков услуг, так и для конечных пользователей. Это горизонтально масштабируемое, экономичное и многофункциональное решение, которое сочетает в себе универсальное хранилище данных с высокопроизводительной виртуализацией.

В этом руководстве описано, как настроить полностью готовый кластер хранилища данных на трех узлах, развернуть поверх него вычислительный кластер и создать виртуальную машину.

2 Аппаратные требования

Минимальная установка Кибер Инфраструктура, рекомендуемая для производственных целей, состоит из трех узлов для сервисов хранения и вычислений с включенной высокой доступностью для узла управления. Это позволяет обеспечить сохранность кластера при отказе одного узла без потери данных. В следующей таблице перечислены *минимальные* аппаратные требования для всех трех узлов. Рекомендуемые конфигурации указаны в разделе «Требования к системе» руководства администратора.

Тип	Узел управления с функциями хранения и вычислений
ЦП	64-разрядные процессоры x86 с включенными аппаратными расширениями виртуализации AMD-V или Intel VT. 16 ядер*
ОЗУ	32 ГБ
Хранилище	1 диск: система + метаданные, жесткий диск SATA 100+ ГБ 1 диск: хранилище, жесткий диск SATA, размер по необходимости
Сеть	10 GbE для трафика хранилища 1 GbE для прочего трафика

*Ядро ЦП здесь означает физическое ядро в многоядерном процессоре (гиперпоточность не учитывается).

3 Установка Кибер Инфраструктура

Внимание

Необходимо синхронизировать время посредством NTP на всех серверах одного кластера. Убедитесь, что все серверы имеют доступ к серверу NTP.

Чтобы установить продукт Кибер Инфраструктура, выполните следующие действия.

1. Получите ISO-образ дистрибутива. Для этого зайдите на [страницу продукта](#) и отправьте запрос на пробную версию. ISO-образ также можно скачать из Кибер Бэкап Облачный.
 - a. Перейдите на портал управления и выберите **НАСТРОЙКИ > Хранилища** в меню слева.
 - b. Нажмите **Добавить хранилище резервных копий** и в открывшемся окне нажмите кнопку **Загрузить ISO-образ**.
2. Подготовьте загрузочный носитель с помощью ISO-образа дистрибутива (подключите его к виртуальному диску IPMI, создайте загрузочный USB-накопитель или настройте PXE-сервер).
3. Загрузите сервер с выбранного носителя.
4. На экране приветствия выберите **Установить Кибер Инфраструктура**.
5. На шаге 1 внимательно прочитайте лицензионное соглашение с конечным пользователем. Примите условия, установив флажок **Я принимаю лицензионное соглашение с конечным пользователем**, и нажмите кнопку **Далее**.
6. На шаге 2 настройте статический IP-адрес для сетевого интерфейса и укажите имя хоста: либо полное доменное имя (**<имя_хоста>.<имя_домена>**), либо краткое имя (**<имя_хоста>**). Не рекомендуется использовать динамический IP-адрес, поскольку это может вызвать проблемы с доступом к серверам. Проверьте правильность сетевых настроек.
7. На шаге 3 выберите часовой пояс. Дата и время будут заданы посредством NTP. Для выполнения синхронизации потребуется подключение к Интернету.
8. На шаге 4 укажите тип устанавливаемого сервера. Сначала разверните один первичный сервер. Затем разверните нужное количество вторичных серверов.
 - Если вы развертываете первичный сервер, выберите два сетевых интерфейса: один для настройки и управления системными сервисами и один для доступа к панели администрирования. Также создайте и подтвердите пароль для учетной записи суперадминистратора панели администрирования. Этот сервер будет сервером управления.
 - Если вы развертываете вторичный сервер, укажите IP-адрес сервера управления и токен. И то и другое можно получить из панели администрирования. Войдите на панель администрирования через порт 8888. IP-адрес панели отображается в консоли после развертывания первичного сервера. Введите имя пользователя по умолчанию **admin** и пароль учетной записи суперадминистратора. На панели администрирования откройте раздел **Инфраструктура > Серверы** и нажмите **Подключить сервер**, чтобы вызвать экран с адресом сервера управления и токеном.

Сервер может появиться на экране **Инфраструктура > Серверы** со статусом **Без назначения** сразу после проверки токена. Однако его можно будет присоединить к кластеру хранения только после завершения установки.

9. На шаге 5 выберите диск для операционной системы. Диску будет назначена дополнительная роль **Система**, хотя вы все равно сможете настроить его для хранения данных на панели администрирования. Также можно создать программный массив RAID1 для системного диска, чтобы обеспечить его высокую производительность и доступность.
10. На шаге 6 введите и подтвердите пароль для учетной записи пользователя root и нажмите **Начать установку**.

После завершения установки сервер автоматически перезагрузится. IP-адрес панели администрирования будет отображен в строке приветствия.

4 Создание кластера хранилища данных

Для создания кластера хранилища выполните следующие действия.

1. Откройте экран **Инфраструктура > Серверы** и нажмите **Создать кластер хранилища**.
2. Введите имя для кластера. Имя может содержать только буквы латинского алфавита (a-z, A-Z), цифры (0-9) и дефисы (-).
3. [Необязательно] Чтобы настроить роли дисков или расположение сервера, нажмите значок шестерни.
4. При необходимости включите шифрование.
5. Нажмите кнопку **Создать**.

Отслеживать создание кластера можно на экране **Инфраструктура > Серверы**. Создание может занять некоторое время в зависимости от количества настраиваемых дисков. Кластер будет создан после завершения настройки.

Чтобы добавить дополнительные узлы в кластер хранилища, выполните следующие действия.

1. На экране **Инфраструктура > Серверы** щелкните по неназначенному серверу.
2. На правой панели сервера нажмите **Присоединить к кластеру**.
3. Нажмите **Присоединить**, чтобы автоматически назначить роли дискам и добавить сервер в текущее расположение. Вместо этого можно нажать значок шестерни, чтобы вручную настроить роли дисков или расположение сервера.

5 Включение высокой доступности сервера управления

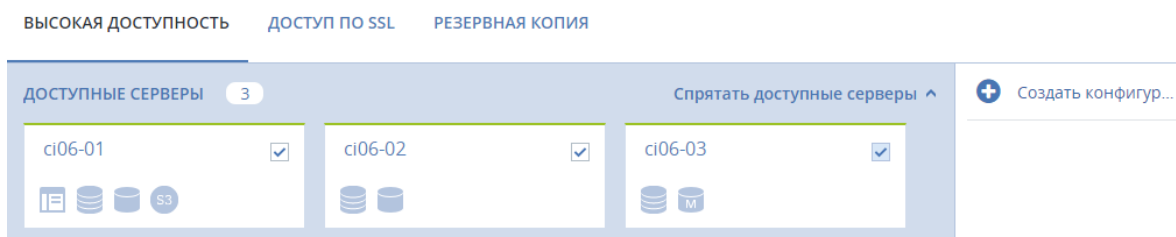
Чтобы сделать инфраструктуру более устойчивой и избыточной, можно создать конфигурацию высокой доступности из трех узлов.

Высокая доступность узла управления и вычислительный кластер тесно связаны, поэтому изменение узлов в одной составляющей обычно влияет на другую. Обратите внимание на следующее:

- Все узлы в конфигурации высокой доступности будут добавлены в вычислительный кластер.
- Одиночные узлы нельзя удалить из вычислительного кластера, так как они включены в конфигурацию высокой доступности. В таком случае вычислительный кластер можно полностью разрушить, но конфигурация высокой доступности останется. Истинно и обратное: конфигурацию высокой доступности можно удалить, а вычислительный кластер продолжит работать.

Чтобы включить высокую доступность для сервера управления и панели администрирования, выполните следующие действия.

1. На экране **Настройки > Сервер управления** откройте вкладку **Высокая доступность**.



2. Выберите три, пять или семь серверов и нажмите **Создать конфигурацию высокой доступности**. Сервер управления будет выбран автоматически.

Примечание

При использовании конфигурации, состоящей из семи серверов, загрузка ЦП и потребление памяти на 25 % выше, чем при использовании конфигурации, состоящей из трех серверов.

3. На шаге **Настройте сеть** убедитесь, что на каждом сервере выбраны правильные сетевые интерфейсы. Если это не так, щелкните по значку шестерни для сервера и назначьте его сетевым интерфейсам сети с типами трафика **Управление системными сервисами** и **Панель администрирования**. Нажмите **Продолжить**.
4. На шаге **Настройте сеть** укажите один или несколько уникальных статических IP-адресов для панели администрирования с высокой доступностью, конечной точки API вычислений и обмена сообщениями между сервисами. Нажмите **Готово**.

После того как высокая доступность сервера управления будет включена, можно выполнить вход на панель администрирования по указанному статическому IP-адресу (на том же порту 8888).

6 Развертывание вычислительного кластера

Перед созданием вычислительного кластера убедитесь, что выполнены следующие требования.

- Сетям назначены типы трафика **ВМ внутр.**, **ВМ внешн.**, **API вычислений** и **Резервные копии ВМ**. Полная рекомендуемая сетевая конфигурация описана в разделе «Настройка сетей для вычислительного кластера» руководства администратора.
- Узлы, добавляемые в вычислительный кластер, подключены к этим сетям и к одной и той же сети с типом трафика **ВМ внешн.**
- На узлах, добавляемых в вычислительный кластер, должна быть одна и та же модель ЦП (см. раздел «Настройка режима эмуляции ЦП для вычислительного кластера» в Руководстве администратора).
- (Рекомендуется) Включена высокая доступность для узла управления (см. раздел "Включение высокой доступности сервера управления" (стр. 9)).

Чтобы создать вычислительный кластер, выполните следующие действия:

1. Откройте экран **Вычисления** и нажмите **Создать вычислительный кластер**.
2. На шаге **Серверы** добавьте серверы в вычислительный кластер:
 - a. Выберите серверы для добавления в вычислительный кластер. Можно выбрать только серверы с состоянием сети **Настроено**. Серверы в кластере высокой доступности сервера управления автоматически выбираются для присоединения к вычислительному кластеру.
 - b. Если сетевые интерфейсы серверов не настроены, щелкните по значку шестерни, выберите необходимые сети и нажмите **Применить**.
 - c. Нажмите кнопку **Далее**.

Настроить вычислительный кластер ✕

- Серверы
- Эмуляция процессора ВМ
- Физическая сеть
- Режим высокой доступности
- Дополнительные сервисы
- Сводка

Выберите серверы для добавления к вычислительному кластеру.

Поиск

<input checked="" type="checkbox"/>	Имя ↑	Статус се...	IP-адрес	Состояние сети
<input checked="" type="checkbox"/>	nod... ⓘ	Исправен	10.77.148.28	<input checked="" type="checkbox"/> Настроено
<input checked="" type="checkbox"/>	node002	Исправен	10.77.148.107	<input checked="" type="checkbox"/> Настроено
<input checked="" type="checkbox"/>	node003	Исправен	10.77.148.17	<input checked="" type="checkbox"/> Настроено

3. На шаге **Эмуляция процессора VM** выполните следующие действия:

- а. Выберите режим эмуляции ЦП виртуальных машин. Режим эмуляции ЦП определяет, какая модель будет назначена и какие дополнительные функции будут доступны виртуальному ЦП.

Режим эмуляции ЦП, заданный на уровне вычислительного кластера, используется по умолчанию для создаваемых VM. При необходимости его можно переопределить на уровне VM.

- **Host-model** (по умолчанию) – модель и набор дополнительных функций виртуального ЦП подбираются таким образом, чтобы они наиболее точно соответствовали модели и дополнительным функциям ЦП вычислительного сервера, на котором размещена виртуальная машина (полное соответствие не гарантируется). Этот режим обеспечивает меньший уровень производительности и безопасности, чем режим **host-passthrough**, но предоставляет большую степень работоспособности горячих миграций виртуальных машин в случае, когда на вычислительных серверах используются незначительно отличающиеся модели ЦП.
- **Host-passthrough** – виртуальной машине предоставляется виртуальный ЦП такой же модели и с такими же дополнительными функциями, как у ЦП вычислительного сервера, на котором размещена виртуальная машина. Этот режим обеспечивает наибольший уровень производительности и безопасности, но не гарантирует работоспособность горячих миграций виртуальных машин при использовании разных моделей ЦП на вычислительных серверах.
- **Custom** – виртуальной машине предоставляется виртуальный ЦП указанной модели с указанными дополнительными функциями. Модель ЦП выбирается из списка моделей ЦП, совместимых со всеми вычислительными серверами (аналогично для дополнительных функций). Этот режим обеспечивает наименьший уровень производительности и безопасности, но гарантирует работоспособность горячих миграций виртуальных машин, даже если на вычислительных серверах используются разные модели ЦП.

Модели ЦП в списке отсортированы по новизне в порядке убывания. По умолчанию все дополнительные функции выбранной модели ЦП отключены.

Некоторые модели ЦП представлены в двух вариантах (например, **Skylake-Server** и **Skylake-Server-IBRS**). Наличие строки "IBRS" в названии модели ЦП означает, что включена защита от аппаратных уязвимостей Spectre и Meltdown. Хотя наличие этой защиты снижает производительность ЦП, в целях безопасности рекомендуется использовать модели ЦП с включенной защитой. Для доверенных приложений возможно

использование моделей ЦП с отключенной защитой.

Custom

При выборе режима виртуализации ЦП "Custom", вы можете явно указать модель ЦП. Список моделей ЦП содержит только модели, совместимые со всеми узлами вычислительного кластера. Выбрав этот режим, вы можете быть уверены, что живые миграции между узлами вычислительного кластера всегда будут возможны.

Выберите модель ЦП
Cascadelake-Server

Выберите дополнительные функции ЦП
pdpe1gb, md-clear, stibp

- b. Включите или отключите поддержку вложенной виртуализации. Её следует включить, если необходима возможность создавать виртуальные машины внутри виртуальных машин. Для модели ЦП qemu64 вложенная виртуализация не поддерживается.
- c. Нажмите кнопку **Далее**.

Настроить вычислительный кластер ✕

- Серверы**
- Эмуляция процессора VM
- Физическая сеть
- Режим высокой доступности
- Дополнительные сервисы
- Сводка

Укажите параметры виртуализации ЦП

Выберите режим виртуализации ЦП

Host-model
При выборе режима виртуализации ЦП "Host-model" будет использоваться модель ЦП, которая наиболее точно соответствует ЦП хоста. Не используйте этот режим, если узлы вычислительного кластера охватывают несколько поколений процессоров.

Host-passthrough
При выборе режима виртуализации ЦП "Host-passthrough" будет использоваться модель ЦП хоста без модификаций, что гарантирует соответствие каждой детали ЦП хоста, обеспечивая лучшую производительность. Используйте этот режим только в том случае, если ваши вычислительные узлы имеют очень высокую степень однородности.

Custom
При выборе режима виртуализации ЦП "Custom" вы можете явно указать модель ЦП. Список моделей ЦП содержит только модели, совместимые со всеми узлами вычислительного кластера. Выбрав этот режим, вы можете быть уверены, что живые миграции между узлами вычислительного кластера всегда будут возможны.

[Назад](#) [Далее](#)

4. На шаге **Физическая сеть** выполните следующие действия:

- a. Включите или отключите управление IP-адресами:
- Если управление IP-адресами включено, встроенный DHCP-сервер автоматически назначит VM, подключенным к сети, IP-адреса из пулов IP-адресов, а также задаст для VM настраиваемые DNS-серверы. Кроме того, по умолчанию для всех сетевых портов VM будет включена защита от спуфинга. Каждый сетевой интерфейс VM сможет принимать и отправлять IP-пакеты, только если ему назначены IP- и MAC-адреса. При необходимости

защиту от спуфинга для интерфейса VM можно отключить вручную.

- Если управление IP-адресами отключено, то VM, 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 VM, и ее нельзя будет включить вручную. Это означает, что каждый сетевой интерфейс VM 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.

- Укажите необходимые сведения для физической сети:
 - Выберите сеть инфраструктуры, к которой будет подключена физическая сеть.
 - Выберите тип физической сети: выберите **VLAN** и укажите идентификатор VLAN для создания сети на базе VLAN либо выберите **Нетегированная** (без тега) для создания плоской физической сети.
 - Если вы включили управление IP-адресами, диапазон IP-адресов подсети в формате CIDR будет заполнен автоматически. При необходимости можно указать шлюз. Если оставить поле **Шлюз** пустым, то шлюз будет исключен из сетевых параметров.
- Нажмите кнопку **Далее**.

Настроить вычислительный кластер ×

• Серверы	Укажите CIDR подсети и шлюз для физической сети. <input checked="" type="checkbox"/> Управление IP-адресами ⓘ Физическая сеть Public <input type="radio"/> VLAN <input checked="" type="radio"/> Нетегированная ⓘ CIDR подсети 10.77.148.0/22 Шлюз (необязательно) 10.77.148.1
• Эмуляция процессора VM	
• Физическая сеть	
• DHCP и DNS	
• Режим высокой доступности	
• Дополнительные сервисы	
• Сводка	

Выбранная физическая сеть появится в списке вычислительных сетей на вкладке **Сеть** вычислительного кластера. По умолчанию она будет совместно использоваться всеми будущими проектами. Доступ к сети можно позже отключить на правой панели сети.

5. Если вы включили управление IP-адресами, вы будете перенаправлены на шаг **DHCP и DNS**, где можно настроить сетевые параметры для управления IP-адресами.

- a. Включите или отключите встроенный DHCP-сервер:
- Если DHCP-сервер включен, сетевым интерфейсам VM 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 VM все равно получают 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.
- b. Укажите один или несколько пулов IP-адресов (диапазоны IP-адресов, которые будут автоматически назначаться виртуальным машинам).
- c. 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 VM).
- d. Нажмите **Добавить**.

Настроить вычислительный кластер
✕

- Серверы
- Эмуляция процессора VM
- Физическая сеть
- DHCP и DNS
- Режим высокой доступности
- Дополнительные сервисы
- Сводка

Включите или отключите DHCP и укажите один или несколько пулов IP-адресов для внешней виртуальной сети.

Встроенный сервер DHCP ⓘ

Пулы IP-адресов
+ Добавить

10.77.148.150 — 10.77.148.254 105 адресов доступно
 ✎ 🗑

Серверы DNS
+ Добавить

10.77.29.101
 ✎ 🗑

Назад
Далее

6. На шаге **Режим высокой доступности** выберите режим высокой доступности сервисов блочного хранилища:

- **Active/Active** (по умолчанию) – в случае отказа вычислительного сервера незавершенные операции с блочным хранилищем (например, создание томов VM) будут перенесены с этого сервера на работоспособный сервер; в случае перезагрузки вычислительного сервера незавершенные операции с блочным хранилищем будут возобновлены на исходном сервере.
- **Active/Passive** – в случае отказа вычислительного сервера незавершенные операции с блочным хранилищем (например, создание томов VM) останутся незавершенными; в случае перезагрузки вычислительного сервера незавершенные операции с блочным хранилищем будут возобновлены на исходном сервере.

Для размещения томов VM можно использовать кластер хранилища данных, входящий в состав Кибер Инфраструктуры, СХД Huawei или СХД HPE 3PAR (подробнее об использовании хранилищ см. в разделе «Управление внешними хранилищами» в руководстве администратора). Выбор режима должен быть основан на том, какое хранилище будет использоваться. Если планируется использовать кластер хранилища данных, выберите режим **Active/Active**. Если планируется использовать СХД Huawei или HPE 3PAR, обратитесь к [официальной документации](#) соответствующего драйвера томов, чтобы определить, какой режим следует выбрать.

Настроить вычислительный кластер
✕

- Серверы
- Эмуляция процессора VM
- Физическая сеть
- DHCP и DNS
- Режим высокой доступности
- Дополнительные сервисы
- Сводка

Выберите режим высокой доступности сервисов блочного хранилища

Active/Active

В режиме высокой доступности "Active/Active" запущенные операции с блочным хранилищем будут завершены успешно как при перезагрузке узла, так и при его отказе. В этом режиме доступно Кибер Хранилище для хранения томов виртуальных машин.

Active/Passive

В режиме высокой доступности "Active/Passive" запущенные операции с блочным хранилищем будут завершены успешно в случае перезагрузки узла, но будут завершены неуспешно при его отказе. В этом режиме недоступно Кибер Хранилище для хранения томов виртуальных машин.

Назад
Далее

7. На шаге **Дополнительные сервисы** включите сервисы, которые будут установлены во время развертывания вычислительного кластера. Эти сервисы также можно установить позже. Затем нажмите кнопку **Далее**.

Примечание

- При установке Kubernetes также автоматически устанавливается сервис балансировщика нагрузки.
- Для автономной установки Kubernetes и сервиса балансировщика нагрузки в среде без доступа к Интернету (в закрытом контуре) необходимо заранее установить на узлы пакеты `hci-k8saas-files` и `amphora-x64-haproxy.qcow2`.

Настроить вычислительный кластер



- Серверы
- Эмуляция процессора VM
- Физическая сеть
- DHCP и DNS
- Режим высокой доступности
- **Дополнительные сервисы**
- Сводка

Дополнительные сервисы

Вы можете установить дополнительные сервисы для вычислительного кластера.

Сервис Kubernetes

Данный сервис позволяет разворачивать готовые к внедрению масштабируемые кластеры Kubernetes с постоянным хранилищем данных.

Разрешите доступ к этим сервисам:

- сервису обнаружения компонента etcd (<https://discovery.etcd.io>) — со всех серверов управления и из публичной сети с типом трафика **VM public**,
- публичному репозиторию Docker Hub (<https://registry-1.docker.io>) — из публичной сети с типом трафика **VM public**,
- вычислительному API-интерфейсу — из публичной сети с типом трафика **VM public**.

Если вычислительный API-интерфейс недоступен из этой сети, но достигаем через NAT, назначьте ему DNS-имя как указано в разделе "Setting a DNS Name for the Compute API" в [Руководство администратора по работе с командной строкой](#).

[Назад](#) [Далее](#)

Настроить вычислительный кластер



- Серверы
- Эмуляция процессора VM
- Физическая сеть
- DHCP и DNS
- Режим высокой доступности
- **Дополнительные сервисы**
- Сводка

Дополнительные сервисы

Если вычислительный API-интерфейс недоступен из этой сети, но достигаем через NAT, назначьте ему DNS-имя как указано в разделе "Setting a DNS Name for the Compute API" в [Руководство администратора по работе с командной строкой](#).

Сервис балансировки нагрузки

Данный сервис обеспечивает масштабирование нагрузки и улучшает доступность и защищенность приложений.

Сервис учета ресурсов для биллинга

Данный сервис ведет учет ресурсов, потребляемых конечными пользователями в рамках проектов. Метрики доступны через API-интерфейс Gnocchi.

[Назад](#) [Далее](#)

8. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать кластер**.

Настроить вычислительный кластер ✕

- Серверы
- Эмуляция процессора VM
- Физическая сеть
- DNCP и DNS
- Режим высокой доступности
- Дополнительные сервисы
- Сводка**

Проверьте конфигурацию вычислительного кластера. При необходимости измените ее, вернувшись на предыдущие шаги.	
CIDR подсети	10.77.148.0/22
Шлюз	10.77.148.1
Физическая сеть	Public
DNCP	Включено
Пулы IP-адресов	10.77.148.150 — 10.77.148.254 105 адресов доступно
Серверы DNS	10.77.29.101
Серверы	node002 (10.77.148.107) node003 (10.77.148.17) node001 (10.77.148.28)
Эмуляция процессора VM	host-model
Режим высокой доступности	Active/Active

[Назад](#) [Создать кластер](#)

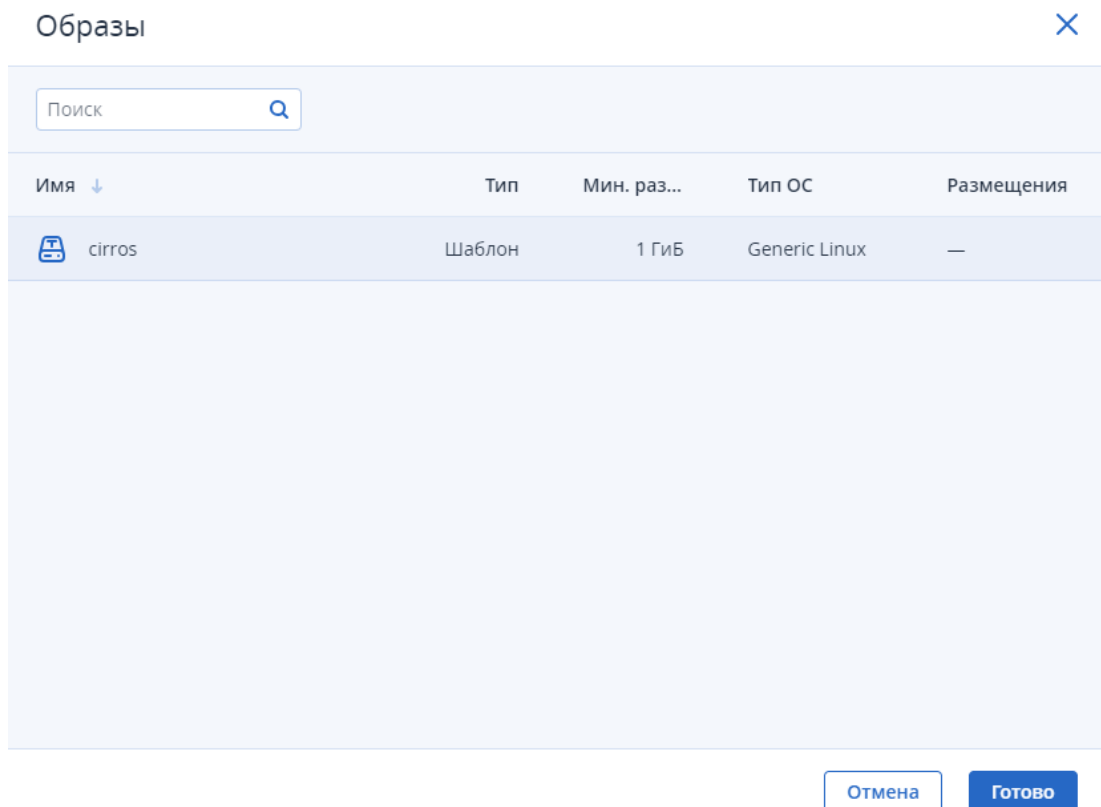
Отслеживать развертывание вычислительного кластера можно на экране **Вычисления**.

7 Создание виртуальной машины

Примечание

Сведения о поддерживаемых гостевых операционных системах и другую информацию см. в разделе «Управление виртуальными машинами» в руководстве администратора.

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



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

Присоединить том



Том
vol1 (6f353ef9-2849-499a-b551-eb0052aa1bbb), 10 ГиБ ▼

Отмена

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.

Тип VM



Поиск <input type="text"/>			
Имя ↓	вЦП ↓	Память	Размещение
tiny	1	512 МиБ	—
small	1	2 ГиБ	—
medium	2	4 ГиБ	—
large	4	8 ГиБ	—
xlarge	8	16 ГиБ	—

6. Добавьте сетевые интерфейсы для VM в разделе **Сети**.
 - а. В окне **Сетевые интерфейсы** нажмите **Добавить**, чтобы присоединить сетевой интерфейс.
 - б. 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 VM. 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.

Добавить сетевой интерфейс ✕

Сеть
net1: 10.10.10.0/24 ▼

MAC-адрес
Автоматически Назначить автоматически

Основной IP-адрес ⓘ + Добавить

IPv4: Назначить автом... 🗑

Дополнительные IP-адреса ⓘ

+ Добавить

Группы безопасности
default ▼

Защита от спуфинга

Невозможно настроить защиту от спуфинга, если выбрана хотя бы одна группа безопасности.

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

- [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.
- Завершив настройку сетевых интерфейсов ВМ, нажмите **Готово**.

Примечание

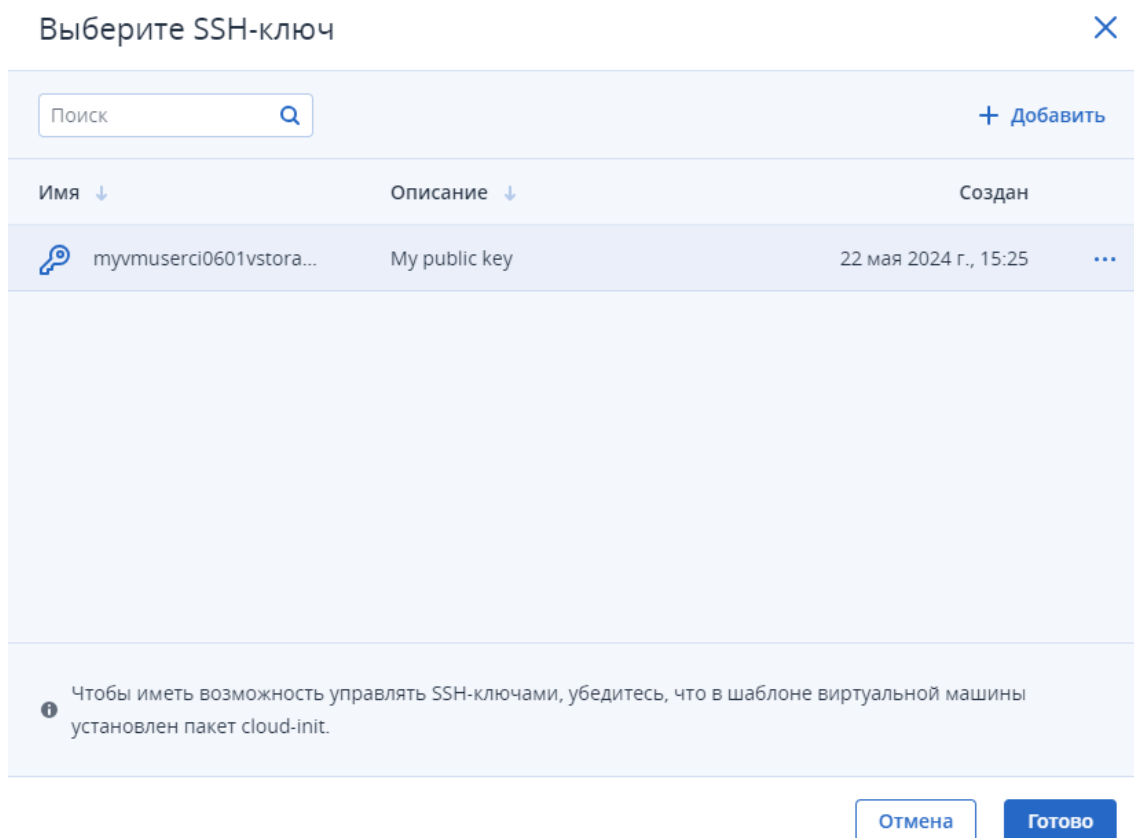
Включите EUI-64 в сетевых настройках VM для корректного назначения IP-адреса.

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 VM, развернутым из этих образов, можно получить только с помощью метода аутентификации с ключом SSH.

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



- Добавьте пользовательские данные для настройки VM 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.

Задайте скрипт настройки



Задайте пользовательские данные для настройки виртуальной машины после запуска. Пользовательские данные могут быть в одном из двух форматов: cloud-config или shell-скрипт. Для возможности настройки гостевой ОС в ее шаблоне должен быть установлен пакет cloud-init.

```
Скрипт настройки
# cloud-config
user: myuser
password: password
chpasswd: {expire: False}
ssh_pwauth: True
```

Загрузить из файла
user-data

Обзор

Отмена

Сохранить

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] Задайте режим эмуляции ЦП виртуальной машины.

Примечание

Если раздел **Режим эмуляции ЦП** не отображается, значит, возможность настройки режима эмуляции ЦП отключена в вашем проекте. Чтобы включить ее, обратитесь к системному администратору.

Режим эмуляции ЦП определяет, какая модель будет назначена и какие дополнительные функции будут доступны виртуальному ЦП. По умолчанию используется режим, заданный на уровне вычислительного кластера. Чтобы использовать другой режим, выполните следующее:

- а. Нажмите на значок карандаша в разделе **Режим эмуляции ЦП**.
- б. В окне **Режим эмуляции ЦП** установите переключатель **Использовать персональные настройки** в положение «вкл» и выберите нужный режим:
 - **Host-model** (по умолчанию) – модель и набор дополнительных функций виртуального ЦП подбираются таким образом, чтобы они наиболее точно соответствовали модели и дополнительным функциям ЦП вычислительного сервера, на котором размещена виртуальная машина (полное соответствие не гарантируется). Этот режим обеспечивает меньший уровень производительности и безопасности, чем режим `host-passthrough`, но предоставляет большую степень работоспособности горячих миграций виртуальных машин в случае, когда на вычислительных серверах используются незначительно

отличающиеся модели ЦП.

- **Host-passthrough** – виртуальной машине предоставляется виртуальный ЦП такой же модели и с такими же дополнительными функциями, как у ЦП вычислительного сервера, на котором размещена виртуальная машина. Этот режим обеспечивает наибольший уровень производительности и безопасности, но не гарантирует работоспособность горячих миграций виртуальных машин при использовании разных моделей ЦП на вычислительных серверах.
- **Custom** – виртуальной машине предоставляется виртуальный ЦП указанной модели с указанными дополнительными функциями. Модель ЦП выбирается из списка моделей ЦП, совместимых со всеми вычислительными серверами (аналогично для дополнительных функций). Этот режим обеспечивает наименьший уровень производительности и безопасности, но гарантирует работоспособность горячих миграций виртуальных машин, даже если на вычислительных серверах используются разные модели ЦП.

Модели ЦП в списке отсортированы по новизне в порядке убывания. По умолчанию все дополнительные функции выбранной модели ЦП отключены.

Некоторые модели ЦП представлены в двух вариантах (например, Skylake-Server и Skylake-Server-IBRS). Наличие строки "IBRS" в названии модели ЦП означает, что включена защита от аппаратных уязвимостей Spectre и Meltdown. Хотя наличие этой защиты снижает производительность ЦП, в целях безопасности рекомендуется использовать модели ЦП с включенной защитой. Для доверенных приложений возможно использование моделей ЦП с отключенной защитой.

Custom

При выборе режима виртуализации ЦП "Custom", вы можете явно указать модель ЦП. Список моделей ЦП содержит только модели, совместимые со всеми узлами вычислительного кластера. Выбрав этот режим, вы можете быть уверены, что живые миграции между узлами вычислительного кластера всегда будут возможны.

Выберите модель ЦП
Cascadelake-Server

Выберите дополнительные функции ЦП
pdpe1gb, md-clear, stibp

с. Нажмите **Применить**.

9. [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.

10. 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.