Пользователи и роли (IAM)

Типы и роли пользователей

Права доступа пользователей разграничиваются через:

- типы пользователей, которые определяют, где будет использоваться учетная запись — в панели управления или для авторизованного доступа через API и инструменты автоматизации;
- роли, которые определяют доступы в рамках каждого типа пользователей.

Добавлять и редактировать пользователей могут только пользователи с ролью Владелец аккаунта или Администратор пользователей.

Вы также можете добавлять пользователей в группы, чтобы управлять несколькими пользователями как одним.

Типы и роли пользователей временно не поддерживаются в следующих группах продуктов и сервисов:

- облако на базе VMware: публичное облако на базе VMware, аварийное восстановление в облако на базе VMware и другие;
- сетевые сервисы (кроме CDN и DNS);
- дополнительные сервисы: мониторинг и другие.

В объектном хранилище доступ пользователя к контейнеру может быть изменен в соответствии с политикой доступа, подробнее в инструкции Управлять доступом в объектное хранилище.

Работать с пользователями и ролями можно в панели управления, с помощью IAM API или Terraform.

Типы пользователей

Тип пользователя указывается при добавлении пользователя и не может быть изменен:

- пользователь панели управления — пользователь с учетной записью в панели управления, который регистрируется в панели управления и при авторизации проходит двухэтапную аутентификацию через почту и номер телефона. Может выписывать себе токен Selectel (ключ API) для полного доступа к API продуктов Selectel;
- сервисный пользователь — пользователь с учетной записью для программного доступа через API продуктов Selectel и другие инструменты автоматизации. Имеет только логин и пароль. Не имеет доступа к панели управления;
- федеративный пользователь — пользователь панели управления, который относится к одной из федераций и проходит аутентификацию через SSO. Не проходит двухэтапную аутентификацию. Пользователь добавляется уже зарегистрированным — ему нужно только ввести ФИО при первом входе. Обязательна почта. Не имеет доступа к API.

Подробнее об авторизации пользователей разных типов в API в инструкции Авторизация документации API.

Роли

В зависимости от типа пользователя ему можно назначить одну или несколько ролей.

Роль можно назначить индивидуально пользователю или группе пользователей.

Посмотрите возможности пользователей с ролями в таблице Сравнение ролей.

Работа с пользователями

Добавить пользователя

Добавлять пользователей могут Владелец аккаунта и Администратор пользователей.

Можно создать пользователя для доступа к панели управления или сервисного пользователя для программного доступа, подробнее в инструкции Типы и роли пользователей.

Если при добавлении пользователя возникли проблемы, создайте тикет.

Добавить пользователя панели управления

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Нажмите **Добавить пользователя**.
3. Выберите тип **Пользователь панели управления**.
4. Введите почту пользователя.
5. Выберите роль пользователя. Для добавления пользователей с ролью Администратор аккаунта или Администратор проекта на балансе аккаунта должно быть минимум 100 ₽.
6. Если вы выбрали роль Администратор проекта или Наблюдатель проекта, отметьте нужные проекты.
7. Опционально: чтобы назначить пользователю еще одну роль, нажмите **Добавить роль** и выберите нужную.
8. Опционально: выберите группу для пользователя.
9. Опционально: отметьте категории уведомлений, которые будут приходить пользователю.
10. Нажмите **Добавить пользователя**. Пользователь будет добавлен в список на вкладке **Пользователи панели управления** со статусом `Не активирован`.
11. Пользователю на электронную почту будет отправлена ссылка для регистрации по приглашению. Учетная запись активируется после подтверждения почты и завершения регистрации.

Добавить сервисного пользователя

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Нажмите **Добавить пользователя**.
3. Выберите тип **Сервисный пользователь**.
4. Введите имя пользователя. Оно будет использоваться при авторизации.
5. Введите пароль для пользователя или сгенерируйте его. После создания пользователя посмотреть пароль нельзя — можно только сгенерировать новый. Пароль должен быть не короче восьми символов и содержать латинские буквы разных регистров и цифры.
6. Выберите роль пользователя. Для добавления пользователей с ролью Администратор аккаунта или Администратор проекта на балансе аккаунта должно быть минимум 100 ₽.
7. Если выбрана роль Администратор проекта, Наблюдатель проекта, Администратор объектного хранилища или Пользователь объектного хранилища, отметьте нужные проекты.
8. Опционально: чтобы назначить пользователю еще одну роль, нажмите **Добавить роль** и выберите нужную.
9. Опционально: выберите группу для пользователя.
10. Нажмите **Добавить пользователя**. Он будет добавлен в список на вкладке **Сервисные пользователи**. Учетная запись будет активна сразу.

Посмотреть идентификатор сервисного пользователя

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Откройте вкладку **Сервисные пользователи**.
3. В строке с пользователем посмотрите значение поля **UID**.

Изменить данные или роль пользователя

Информация об аккаунте и пользователе содержится в профиле. Набор данных в профиле зависит от типа аккаунта и роли пользователя. Посмотреть свой профиль можно в панели управления в разделе **Профиль и настройки**.

Владельцу аккаунта и Администратору пользователей доступна информация обо всех пользователях в панели управления в разделе **Управление доступом** → **Управление пользователями**. Владелец аккаунта и Администратор пользователей могут изменять некоторые данные пользователей:

Чтобы изменить номер телефона, адрес электронной почты, ФИО, реквизиты компании, измените данные профиля.

Данные федеративных пользователей не хранятся в Selectel, их можно изменить на стороне вашего Identity Provider.

Изменить Владельца аккаунта

Если у вас бизнес-аккаунт, чтобы изменить Владельца аккаунта, который является контактным лицом, создайте тикет.

Если у вас личный аккаунт, сделать Владельцем аккаунта другого человека нельзя — можно зарегистрировать новый аккаунт и перенести на него услуги.

Изменить имя сервисного пользователя

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Откройте вкладку **Сервисные пользователи**.
3. В меню ⁝ пользователя нажмите **Редактировать**.
4. Внесите изменения.
5. Нажмите **Сохранить**.

Изменить пароль сервисного пользователя

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Откройте вкладку **Сервисные пользователи**.
3. В меню ⁝ пользователя нажмите **Изменить пароль**.
4. Введите новый пароль или нажмите **Сгенерировать**.
5. Нажмите **Изменить пароль**.

Изменить роль пользователя

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Откройте вкладку с нужным типом пользователей.
3. В меню ⁝ пользователя нажмите **Редактировать**.
4. Измените роль.
5. Нажмите **Сохранить**.

Изменить проекты пользователя

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Откройте вкладку с нужным типом пользователей.
3. В меню ⁝ пользователя нажмите **Редактировать**.
4. Измените проекты пользователя.
5. Нажмите **Сохранить**.

Изменить группы пользователя

Добавить пользователя в группу

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.

2. Откройте вкладку с нужным типом пользователей.
3. Откройте страницу пользователя → вкладка **Группы**.
4. Нажмите **Добавить в группу**.
5. Выберите группы.
6. Нажмите **Добавить**.

Исключить пользователя из группы

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Откройте вкладку с нужным типом пользователей.
3. Откройте страницу пользователя → вкладка **Группы**.
4. В строке с группой, из которой хотите исключить пользователя, нажмите 🗑️.
5. Введите имя группы для подтверждения.
6. Нажмите **Исключить**.

Изменить категории уведомлений пользователя

Используйте инструкцию Уведомления аккаунта.

Отключить или удалить пользователя

Отключать и удалять пользователей могут Владелец аккаунта и Администратор пользователей.

Пользователя панели управления можно только удалить. Сервисного пользователя можно отключить или удалить.

Удалить пользователя

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Откройте вкладку с нужным типом пользователей.
3. В меню ⋮ пользователя нажмите **Удалить**.
4. Введите почту пользователя для подтверждения.
5. Нажмите **Удалить**.

Отключить сервисного пользователя

Отключенный пользователь не сможет авторизоваться под своими учетными данными. Включить пользователя можно в любой момент.

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Откройте вкладку **Сервисные пользователи**.
3. В строке с пользователем выключите тумблер.

Группы пользователей

В панели управления есть возможность объединять пользователей в группы. С помощью группы можно централизованно управлять несколькими пользователями — назначать роль группе, а не каждому пользователю индивидуально. Каждый пользователь в группе будет наследовать эти роли. Например, можно объединить пользователей для управления определенным проектом или биллингом.
В группу можно добавлять пользователей разных типов. Один пользователь может быть добавлен в несколько групп. Если до добавления в группу у пользователя были другие роли (индивидуальные или роли другой группы), они суммируются с ролями группы.

Создать и настроить группу пользователей

1. Создайте группу.
2. Назначьте роли группе.
3. Добавьте пользователей в группу.

1. Создать группу

1. В панели управления перейдите в раздел **Управление доступом** → **Группы пользователей**.
2. Нажмите **Добавить группу**.
3. Введите имя группы.
4. Опционально: введите описание группы.
5. Нажмите **Добавить группу**.

2. Назначить роли

1. В панели управления перейдите в раздел **Управление доступом** → **Группы пользователей**.
2. Откройте страницу группы пользователей.
3. В блоке **Роли** нажмите **Назначить роль**.
4. Выберите роль. Для добавления роли Администратор аккаунта или Администратор проекта на балансе аккаунта должно быть минимум 100 ₽.
5. Если вы выбрали роль Администратор проекта или Наблюдатель проекта, отметьте нужные проекты.
6. Опционально: чтобы назначить группе еще одну роль, нажмите **Добавить роль** и выберите нужную.

3. Добавить пользователей в группу

1. В панели управления перейдите в раздел **Управление доступом** → **Группы пользователей**.
2. Откройте страницу группы пользователей.
3. В блоке **Пользователи** нажмите **Добавить пользователей**.
4. В списке всех пользователей в аккаунте отметьте пользователей, которых хотите добавить в группу.

5. Нажмите **Сохранить**.

Изменить группу пользователей

Вы можете изменять имя группы, изменять роли, добавлять новых пользователей в группу, исключать пользователей из группы.

Изменить имя и описание группы

1. В панели управления перейдите в раздел **Управление доступом** → **Группы пользователей**.
2. Откройте страницу группы пользователей.
3. В меню ⋮ группы выберите **Редактировать название и описание**.
    - Измените имя и описание группы.
    - Нажмите **Сохранить**.

Изменить роли группы

1. В панели управления перейдите в раздел **Управление доступом** → **Группы пользователей**.
2. Откройте страницу группы пользователей.
3. В блоке **Роли** нажмите **Редактировать**.
4. Чтобы удалить роль, в строке с ролью нажмите 🗑️.
5. Чтобы добавить роль, нажмите **Добавить роль** и выберите роль. Для добавления роли Администратор аккаунта или Администратор проекта на балансе аккаунта должно быть минимум 100 ₽.
6. Если вы выбрали роль Администратор проекта или Наблюдатель проекта, отметьте нужные проекты.
7. Опционально: чтобы назначить группе еще одну роль, нажмите **Добавить роль** и выберите нужную.

Исключить пользователей из группы

При исключении пользователя из группы пользователь не удаляется, но из списка его ролей удаляются роли, которые он имел в этой группе. Если у пользователя есть индивидуальная роль или он состоит в других группах, у него останутся соответствующие роли. Если у пользователя нет других ролей, он останется без роли.

1. В панели управления перейдите в раздел **Управление доступом** → **Группы пользователей**.
2. Откройте страницу группы пользователей.
3. В блоке **Пользователи** в строке с пользователем нажмите 🗑️.
4. Введите имя группы для подтверждения.
5. Нажмите **Исключить**.

Удалить группу пользователей

При удалении группы пользователи не удаляются, но из списка их ролей удаляются роли, которые они имели в этой группе. Если у пользователя есть индивидуальная роль или он состоит в других группах, у него останутся соответствующие роли. Если у пользователя нет других ролей, он останется без роли.

1. В панели управления перейдите в раздел **Управление доступом** → **Группы пользователей**.
2. В меню ⋮ выберите **Удалить**.
3. Введите имя группы для подтверждения.
4. Нажмите **Удалить**.

Федерации

Федерации и федеративные пользователи

Федерации удостоверений позволяют настроить аутентификацию в панели управления с помощью технологии единого входа — Single Sign-On (SSO). При таком способе аутентификации данные пользователей хранятся у вашего поставщика удостоверений — Identity Provider (например, Keycloak, ADFS и другие SAML-совместимые поставщики).

Для работы с федерациями поставщики удостоверений должны поддерживать протокол SAML 2.0.

Вы можете настроить до 10 федераций для доступа через учетные записи разных поставщиков.

Управлять федерациями можно через панель управления и через Federations API.

Федеративные пользователи

Для использования федераций создается отдельный тип пользователей — федеративные, которые являются подтипом пользователей панели управления. Федеративному пользователю можно присвоить те же роли, что и пользователям панели управления.

Федеративные пользователи проходят аутентификацию в панели управления Selectel по SSO так же, как они это делают при входе в корпоративные системы своей организации. При аутентификации пользователь переходит на страницу авторизации у поставщика удостоверений — ему не нужно иметь отдельную учетную запись для Selectel и вводить логин и пароль при каждом входе в панель управления.

Логин и пароль федеративного пользователя не хранится в Selectel.

Федеративный пользователь не имеет доступа к API.

Создать федерацию

1. Если у вас нет сертификата, выпущенного у вашего поставщика удостоверений, выпустите его.
2. Создайте федерацию.
3. Добавьте федеративных пользователей.
4. Настройте федерацию на стороне поставщика удостоверений.

Сертификаты

При работе с федерациями используется два типа сертификатов:

- сертификат поставщиков удостоверений — сертификат, который выпускается на стороне поставщика удостоверений и добавляется при настройке федерации в панели управления. Без сертификата федерация работать не будет;
- сертификаты для подписи запросов — необязательный сертификат, который выпускается на стороне Selectel, если у федерации отмечен чекбокс **Подписывать запросы аутентификации**.

Настроить Keycloak

В результате настройки будет создано SAML-приложение.

1. Настройте SAML-приложение.
2. Если при создании федерации вы отметили чекбокс **Подписывать запросы аутентификации**, в SAML-приложении настройте проверку цифровой подписи.

Настроить AD FS

Настройка AD FS в этой инструкции описана на примере ОС Windows Server 2019, для других версий шаги могут отличаться.

Настраивать Active Directory Federation Services (AD FS) нужно в соответствии с рекомендациями компании Microsoft по развертыванию кластеров и прокси-серверов AD FS.

1. Настройте отношения доверия.
2. Настройте Claims Mapping.

Аутентификация по SSO

Первая аутентификация

После приглашения в аккаунт федеративный пользователь получит на электронную почту письмо со ссылкой для авторизации по SSO и ID федерации.

1. В письме нажмите **Войти по SSO**.
2. Введите ID федерации.
3. Опционально: чтобы не вводить ID федерации при каждом входе, отметьте чекбокс **Сохранить федерацию**.
4. Нажмите **Войти**.
5. Вы будете перенаправлены на страницу авторизации у поставщика удостоверений. После авторизации вы будете возвращены на страницу входа в панели управления.
6. Введите ФИО.
7. Нажмите **Войти**.

Аутентификация при каждом входе

1. В панели управления на странице входа нажмите **Войти с помощью SSO**.
2. Введите ID федерации или выберите сохраненную федерацию. ID федерации можно посмотреть в письме-приглашении или запросить у Администратора пользователей.
3. Опционально: чтобы не вводить ID новой федерации при каждом входе, отметьте чекбокс **Сохранить федерацию**.
4. Нажмите **Войти**. Вы будете перенаправлены на страницу авторизации у поставщика удостоверений.
5. Авторизуйтесь у поставщика удостоверений.

Ошибки при аутентификации

Если федерация была настроена некорректно, при аутентификации федеративного пользователя могут возникать ошибки. Группы ошибок:

- SAML001 — SAML099 — ошибки конфигурации федерации на стороне Selectel;
- SAML100 — SAML199 — ошибки валидации на стороне поставщика удостоверений (SAML Response);
- SAML200 — SAML299 — остальные ошибки.

Посмотрите причины и способы решения ошибок в таблице Ошибки при аутентификации.

Проекты

Проекты

Проект — группа ресурсов аккаунта, управление которыми можно изолировать на уровне пользователей аккаунта, их типов и ролей. Ресурсы одного проекта могут находиться в разных регионах, зонах доступности и пулах. Для некоторых ресурсов в проекте можно установить ограничение на создание — лимиты проекта и квоты.

В проектах можно управлять ресурсами только тех продуктов, которые поддерживают работу с проектами.

Первый проект (My First project) создается автоматически при регистрации аккаунта в панели управления. Если нужно, удалите этот проект и создайте новый.

Проект нужно выбрать при заказе или создании продукта. После заказа или создания можно перенести ресурсы в другой проект. Длительность переноса зависит от продукта и ресурса, который вы хотите перенести. Например, перенести диски облачной платформы или перенести выделенный сервер вы можете быстро, а перенос облачного сервера займет у вас больше времени.

Управление проектами: типы и роли пользователей

Управлять проектами могут пользователи всех типов:

- пользователи панели управления и федеративные пользователи — через панель управления;
- сервисные пользователи — через API продуктов Selectel и другие инструменты автоматизации: OpenStack CLI, Terraform, selvpc.

Для управления проектом пользователю должна быть назначена роль с доступом в проект. Она определяет, к каким операциям у пользователя есть доступ. Определить, какая роль подходит пользователю, можно в таблице Сравнение ролей при управлении проектами.

Если у пользователя нет доступа к проекту, вы можете добавить его в проект, подробнее в инструкциях Добавить администратора проекта и Добавить наблюдателя проекта.

Лимиты проекта и квоты

В каждом проекте по умолчанию устанавливаются лимиты проекта — ограничения на создание ресурсов облачной платформы. Лимиты проекта можно изменить только через техническую поддержку.

В пределах лимитов проекта пользователи с определенными ролями могут увеличивать или уменьшать квоты на ресурсы в панели управления или через API — подробнее об изменении квот.

Лимиты проекта

В проектах выделяется лимит на каждый ресурс — это максимальное количество ресурса, которое можно создать в одном проекте. Лимиты устанавливаются автоматически при создании проекта.

Лимиты одного ресурса могут отличаться в разных пулах и сегментах пула. По умолчанию лимиты определенного ресурса в одном пуле или сегменте пула одинаковы во всех проектах аккаунта.

Вы можете увеличить лимит любого проекта через техническую поддержку. Для разных проектов можно устанавливать разные лимиты. По мере использования продукта лимиты могут увеличиваться автоматически.

Увеличить лимит проекта

Для разных проектов можно устанавливать разные лимиты.

1. Создайте тикет. Лимиты увеличатся только в одном проекте.
2. Увеличьте квоты.

Квоты

С помощью квот можно ограничить создание облачных ресурсов в проекте — для контроля потребления и ограничения расходов.

Когда количество ресурса достигнет значения квоты, ресурс перестанет создаваться. Например, вы выделили в одном проекте квоту на создание десяти vCPU в сегменте пула ru-7a. Пока вы не увеличите квоту, не создастся больше десяти vCPU. Можно полностью ограничить создание ресурса — выставить квоту, равную нулю.

При создании проекта на каждый ресурс по умолчанию выделяются квоты, равные лимитам проекта. Значения квот одного ресурса могут отличаться в разных пулах и сегментах пула. Можно изменить квоты в рамках лимита проекта.

Неиспользуемые квоты не оплачиваются — вы платите только за используемые ресурсы. Например, если вы выделили квоту на десять публичных IP-адресов, но создали три IP-адреса — будут оплачиваться только три адреса.

Изменить квоты

Значение квоты на каждый ресурс можно увеличить или уменьшить, но только в рамках лимита проекта. Для одного ресурса можно выделить разное количество квот в разных пулах и сегментах пула.

Можно изменить все квоты проекта одновременно: повысить до максимума (лимита проекта) или снизить до текущего потребления.

Квоты можно изменить через Quota Management API или в панели управления.

1. В панели управления перейдите в раздел **Облачная платформа → Квоты**.

2. Выберите регион и пул, в котором нужно изменить квоты.
3. В строке нужной квоты → в столбце **Квота** нажмите □.
4. Укажите новое значение квоты. Значение квоты должно быть не меньше текущего потребления, его можно посмотреть в столбце **Используется**. Если вы достигли максимального значения квоты, увеличьте лимит проекта.
5. Нажмите ✓.
6. Опционально: чтобы повысить все квоты проекта до лимита проекта, в меню ⋮ выберите **Повысить все квоты проекта до максимума**. Чтобы снизить все квоты до текущего потребления, выберите **Снизить все квоты проекта до потребления**.

Посмотреть потребление

Можно посмотреть максимально возможное потребление для текущего количества квот (сколько потратит проект, если будут использованы все квоты) и текущее потребление каждого ресурса и пула.

1. В панели управления перейдите в раздел **Облачная платформа → Квоты**.
2. Посмотрите текущее потребление каждого ресурса в столбце **Потребление**.
3. Чтобы посмотреть максимально возможное потребление проекта, нажмите **Сколько будет потреблять проект, если я использую все выделенные квоты?**

Создать проект

По умолчанию для одного аккаунта можно создать до 20 проектов. Если вам нужно больше проектов, создайте тикет.

1. В панели управления перейдите в раздел продукта.
2. Если в аккаунте еще нет проектов, нажмите **Создать проект** на странице раздела. Если вы создаете проект в разделе **Серверы и оборудование**, вы будете автоматически перенаправлены в раздел **Облачная платформа**.
3. Если в аккаунте уже есть проекты, нажмите на название текущего проекта, выберите **Управление проектами** и нажмите **Создать проект**.
4. Введите имя проекта. Оно должно быть уникальным для аккаунта.
5. Нажмите **Создать проект**. Если вы создавали проект в разделе **Серверы и оборудование**, вернитесь в раздел **Серверы и оборудование**.

Работа с проектами

Переименовать проект

1. В панели управления перейдите в раздел продукта.
2. Нажмите на название текущего проекта и выберите **Управление проектами**. Если вы переименовываете проект в разделе **Серверы и оборудование**, вы будете автоматически перенаправлены в раздел **Облачная платформа**.
3. В меню ⋮ проекта выберите **Переименовать**.

4. Введите новое имя проекта.
5. Нажмите ✓. Если вы переименовывали проект в разделе **Серверы и оборудование**, вернитесь в раздел **Серверы и оборудование**.

Перенести проект в другой аккаунт

Если на аккаунте Selectel уже пополнялся баланс, то переоформить аккаунт на другое юридическое или физическое лицо нельзя. Зарегистрируйте новый аккаунт и перенесите в него все проекты и услуги. В этом случае перенастраивать услуги в новом аккаунте не потребуется.
Можно перенести проект, несколько услуг или все услуги аккаунта. Ограничения:

- если услуги объединены приватной сетью на уровне L3 с помощью глобального роутера, их нельзя перенести по отдельности — только все сразу. В принимающем аккаунте связность между услугами сохранится;
- некоторые услуги переносятся только с даунтаймом — мы предупредим вас в тикете;
- при переносе проекта будут перенесены все ресурсы этого проекта: выделенные серверы, облачные серверы, контейнеры, публичные IP-адреса, базы данных и остальные ресурсы;
- все ресурсы останутся в том же сегменте пула.

Если на передающем аккаунте есть услуги с оплатой по тарифному плану, то при переносе оплаченный период не сохраняется. На баланс передающего аккаунта будут возвращены средства за все неиспользованные дни, а на принимающем аккаунте оплаченный период начнется сразу после переноса.
После возврата средств на передающий аккаунт вы можете оформить возврат денег.
Перенос услуг в другой аккаунт занимает до 15 минут.

Перенести проект

1. Убедитесь, что у вас есть принимающий аккаунт. Если его нет, зарегистрируйте новый аккаунт.
2. Пополните баланс принимающего аккаунта. Баланс должен быть не меньше стоимости переносимых услуг с оплатой по тарифному плану.

   Посмотреть расходы на инфраструктуру можно в панели управления в разделе **Обзор биллинга** → блок **Расходы**.

3. Объедините все ресурсы для переноса в существующем или новом проекте.

   Используйте инструкции по переносу:

   - для выделенных серверов и размещения оборудования;
   - облачного сервера;
   - сетевого диска;
   - образа облачного диска.
4. Перенести ресурсы объектного хранилища в другой проект можно с помощью инструментов для работы с хранилищем.

5. Если нужно перенести сети выделенного сервера и размещаемого оборудования, убедитесь, что вы не используете их с ресурсами, которые останутся на передающем аккаунте. Чтобы посмотреть весь список своих публичных IP-адресов, в панели управления перейдите в раздел **Сетевые сервисы** → **IP-адреса**.
6. Создайте тикеты с запросом на перенос с передающего и принимающего аккаунтов. Тикеты должны создать пользователи с ролью Владелец аккаунта не менее чем за сутки до переноса.

   В тикетах укажите:

   - номера передающего и принимающего аккаунтов;
   - дату и время переноса. Если мы не сможем перенести услуги в указанное время, мы предупредим вас в тикете и согласуем другое время;
   - список ID проектов для переноса: в панели управления перейдите в раздел продукта → нажмите на название текущего проекта → в строке нужного проекта нажмите ⿻;
   - список услуг для переноса, которые не поддерживают работу с проектами.
7. Сообщите в тикете код подтверждения, который мы направим на контактный номер телефона передающего аккаунта.
8. Если нужно перенести оборудование, размещенное в Selectel, мы пришлем в тикетах документы:
   - на передающий аккаунт — акт приема-передачи для возврата оборудования;
   - принимающий аккаунт — акт приема-передачи для приема оборудования и Условия оказания услуг связи.
9. До даты переноса подпишите документы, заверьте печатью и направьте скан-копии в тикете.
10. Когда перенос услуг завершится, мы отправим уведомление в тикете.
11. Убедитесь, что перенос завершен успешно.
12. Опционально: оформите возврат денег, которые остались на передающем аккаунте. Если передающий и принимающий аккаунты оформлены на одно лицо, можно запросить перенос баланса — создайте тикет и укажите номера передающего и принимающего аккаунта. Мы пришлем заявление для переноса баланса.
13. Опционально: добавьте дополнительных пользователей, которые были созданы в передающем аккаунте.

Добавить администратора проекта

Добавить администратора проекта могут пользователи с ролями Владелец аккаунта и Администратор пользователей.

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.
2. Откройте вкладку с нужным типом пользователей:
   - пользователи панели управления и федеративные пользователи — для настройки доступа через панель управления;

    - сервисные пользователи — для настройки доступа через API продуктов Selectel и другие инструменты автоматизации: OpenStack CLI, Terraform, selvpc.
3. Выберите пользователя, который будет администрировать проект.
4. В меню ⁝ пользователя нажмите **Редактировать**.
5. Если у пользователя нет роли Администратор проекта, добавьте ему эту роль.
6. Выберите проекты, которые может администрировать пользователь.
7. Нажмите **Сохранить**.

Добавить наблюдателя проекта

Добавить наблюдателя проекта могут пользователи с ролями Владелец аккаунта и Администратор пользователей.

1. В панели управления перейдите в раздел **Управление доступом → Управление пользователями**.
2. Откройте вкладку с нужным типом пользователей:
    - пользователи панели управления и федеративные пользователи — для настройки доступа через панель управления;
    - сервисные пользователи — для настройки доступа через API продуктов Selectel и другие инструменты автоматизации: OpenStack CLI, Terraform, selvpc.
3. Выберите пользователя, который будет наблюдателем проекта.
4. В меню ⁝ пользователя нажмите **Редактировать**.
1. Если у пользователя нет роли Наблюдатель проекта, добавьте ему эту роль.
2. Выберите проекты, за которыми может наблюдать пользователь.
3. Нажмите **Сохранить**.

Удалить проект

Можно удалить только те проекты, в которых удалены все ресурсы.

1. Убедитесь, что вы удалили все ресурсы в проекте.
2. В панели управления перейдите в раздел раздел продукта.
3. Нажмите на название текущего проекта и выберите **Управление проектами**. Если вы удаляете проект в разделе **Серверы и оборудование**, вы будете автоматически перенаправлены в раздел **Облачная платформа**.
4. В меню ⁝ проекта выберите **Удалить**.
1. Введите имя проекта.
2. Нажмите **Удалить проект**. Если вы удаляли проект в разделе **Серверы и оборудование**, вернитесь в раздел **Серверы и оборудование**.

Облачные серверы

Общая информация

Облачный сервер — это виртуальный сервер, который можно создать на базе ресурсов облачной платформы.

Облачная платформа Selectel — это управляемое публичное облако в одном из пулов. Для работы с облачной платформой нужно создать проект — изолированное облако с ресурсами, которые можно масштабировать.

Работать с облачным сервером можно в панели управления, через OpenStack CLI или Terraform.

В продукте поддерживаются типы и роли пользователей, проекты и лимиты проекта и квоты.

Если вам нужна помощь с администрированием облачных серверов, закажите услуги администрирования сервисов.

Модель оплаты и цены облачного сервера

Баланс

Для оплаты ресурсов облачной платформы в зависимости от типа баланса в аккаунте используется единый баланс или баланс облачной платформы.

Оплатить ресурсы можно разными типами средств: основными средствами, бонусами или ВК бонусами.

Перед оплатой пополните баланс.

Модель оплаты

В облачной платформе используется модель оплаты pay-as-you-go. С баланса каждый час списываются средства за предыдущий час использования ресурсов облачной платформы, а также оплачивается внешний трафик.

Все созданные ресурсы оплачиваются, даже если они выключены.

Например, вы создали облачный сервер с ресурсами: vCPU, RAM и Универсальный диск. Если вы выключите или приостановите облачный сервер, ресурсы продолжат оплачиваться каждый час.

При заморозке сервера не тарифицируются vCPU, RAM и GPU, при этом оплачиваются остальные ресурсы.

Подробнее об оплате в документе Условия использования отдельных сервисов: группа услуг Облачная платформа.

Блокировка ресурсов, если на балансе недостаточно средств

Если на момент списания на балансе будет недостаточно средств для оплаты, то все ресурсы облачной платформы автоматически заблокируются — при этом за них продолжит начисляться плата.

Чтобы восстановить доступ к ресурсам, нужно пополнить баланс на сумму долга в течение 14 дней после блокировки. Долг за ресурсы, которые тарифицировались в период блокировки, автоматически погасится. Проекты не блокируются — можно удалить проект целиком или ресурсы через API.

Если в течение 14 дней после блокировки не пополнить баланс на сумму долга, все ресурсы облачной платформы удалятся. Проекты при этом не удаляются.

Чтобы не пропускать пополнения баланса, вы можете настроить уведомления о состоянии баланса.

Внешний трафик

Внешний трафик — это входящий и исходящий трафик между публичным адресом объекта облачной платформы и публичным адресом в интернете. Остальной трафик относится к внутреннему.

На все проекты в рамках одного аккаунта облачной платформы каждый месяц предоставляются 3 ТБ бесплатного внешнего трафика. После использования бесплатных 3 ТБ внешний трафик оплачивается по модели оплаты облачной платформы.

По умолчанию для облачной платформы включена базовая защита Selectel от DDoS-атак. Вредоносный отфильтрованный DDoS-трафик не учитывается в потреблении и не тарифицируется.

Внутренний трафик

Внутренний трафик — это входящий и исходящий трафик между публичным адресом объекта облачной платформы и публичным адресом другой услуги Selectel, например Выделенный сервер.

Трафик между проектами и пулами облачной платформы Selectel тоже относится к внутреннему.

Со стороны облачной платформы трафик (входящий и исходящий) до любых других услуг Selectel не оплачивается.

Посмотреть потребление

Посмотреть текущую стоимость всей облачной инфраструктуры, потребление и оплату инфраструктуры и внешнего трафика можно в панели управления в разделе **Облачная платформа → Потребление платформы**.

Текущая стоимость

Текущая стоимость — это количество денег, которое потребляет текущая конфигурация облачной инфраструктуры за определенное время.

Текущую стоимость можно посмотреть в панели управления в разделе **Облачная платформа → Потребление платформы →** вкладка **Текущая стоимость**.

Можно посмотреть текущую стоимость определенных проектов, ресурсов и пулов за час, день или месяц.

Данные о стоимости инфраструктуры обновляются каждый час. В панели управления они отображаются на 5–35 минут позже реального изменения инфраструктуры и ее стоимости. Недавно удаленные ресурсы могут продолжать отображаться в панели управления до следующего обновления данных. При этом ресурсы перестают тарифицироваться со следующего часа после удаления.

Графики потребления и оплаты

Графики потребления и оплаты инфраструктуры можно посмотреть в панели управления в разделе **Облачная платформа → Потребление платформы →** вкладка **График расходов →** вкладки **Потреблено** и **Оплачено**.

Можно посмотреть потребление определенных проектов, объектов, ресурсов, регионов и пулов. Графики потребления и оплаты можно посмотреть за определенный период времени или отсортировать по дням, неделям, месяцам, годам.

Чтобы выгрузить детализацию потребления и оплаты в формате `.csv`, нажмите **Скачать CSV** и выберите, как будут сгруппированы строки в выгрузке (по часам, дням, неделям, месяцам, годам).

Все блокировки ресурсов отображаются на графиках потребления и графиках оплаты.

Трафик

Потребление внешнего трафика за текущий месяц можно посмотреть в панели управления в разделе **Облачная платформа → Потребление платформы →** вкладка **Внешний трафик**.

Чтобы выгрузить детализацию потребления внешнего и внутреннего трафика за каждый час по всем публичным адресам аккаунта в формате `.csv`, выберите период и нажмите **Скачать CSV**. Можно выгрузить детализацию только за последние три месяца.

Цены

Цены на ресурсы и внешний трафик можно посмотреть на selectel.ru. Цены в пулах могут различаться.

Рассчитать стоимость облачного сервера можно в калькуляторе ресурсов.

Отчетные документы

После оплаты можно получить отчетные документы.

Приватные сегменты пула

Приватные сегменты пула можно использовать для резервирования одного или нескольких хостов виртуализации — запустить облачные серверы с изоляцией на физическом уровне, если есть особенные требования к безопасности или для гарантии наличия вычислительных ресурсов в любой момент времени.

В публичных сегментах пула облачные серверы работают на физических хостах, которые могут совместно использоваться многими клиентами. Каждый сегмент пула связан с одним или несколькими физическими серверами. Внутри каждого приватного сегмента вы можете полностью контролировать ресурсы облачной платформы, не разделяя оборудование хоста с другими клиентами.

Доступные ресурсы

Приватный сегмент пула можно использовать в любом проекте аккаунта вместе с публичными пулами. Доступ к использованию ресурсов ограничивается лимитами проекта.

В приватном сегменте пула:

- доступны все типы сетевых дисков облачной платформы. Для реализации нестандартных требований к емкости или производительности сетевых дисков можно организовать выделенное сетевое хранилище;
- можно настроить резервное копирование сетевых дисков с помощью бэкапов;
- облачные серверы могут использовать те же сетевые ресурсы, что и в публичных сегментах;
- облачные серверы можно объединить с серверами в других сегментах приватной сетью;
- используются хранилища образов тех сегментов пула, на базе которых они запущены.

Конфигурации

Приватный сегмент пула может состоять из одного или нескольких хостов виртуализации. Использовать несколько разных процессоров в рамках одного сегмента нельзя.

Лимит аккаунта на ресурсы приватного сегмента пула:

- vCPU — 1 vCPU на одно физическое ядро процессора (можно изменить по запросу);
- RAM — сумма емкостей хостов виртуализации;
- локальный диск — сумма емкостей хостов виртуализации.

В приватном сегменте можно запускать облачные серверы только с фиксированными конфигурациями.

Действуют ограничения на максимальный размер облачного сервера — он определяется параметрами хостов виртуализации, входящих в состав сегмента пула. Например, если приватный сегмент пула сформирован из хостов с 36 физическими ядрами и 354 ГБ оперативной памяти, то максимальный размер сервера будет ограничен 36 vCPU и 354 ГБ RAM.

Обслуживание хостов виртуализации в приватных сегментах пула выполняется специалистами Selectel.

Процессоры

Посмотреть доступность процессоров в регионах можно в матрице доступности Приватные сегменты пула.

Подключить приватный сегмент пула

Для подключения приватного сегмента пула создайте тикет.

Создание приватного сегмента пула с количеством хостом до четырех хостов занимает один рабочий день, от пяти хостов — от одной недели.

Перенос ресурсов в приватный сегмент пула из публичного можно выполнить самостоятельно — создать диск из снапшота или образа.

Стоимость

Приватные сегменты пула оплачиваются по модели оплаты облачной платформы.

Стоимость приватного сегмента пула зависит от выбранной конфигурации хостов виртуализации и их количества — учитывается количество физических ядер, количество памяти и объем локального диска.

Точную стоимость мы предоставим в ответе на тикет.

Создать облачный сервер

Конфигурации облачных серверов

При создании облачного сервера можно выбрать количество vCPU, RAM, размер локального диска (опционально) и добавить графические процессоры.

Доступно два типа конфигураций:

- фиксированные конфигурации — несколько линеек с разными техническими характеристиками, в которых зафиксировано соотношение ресурсов;
- произвольные конфигурации, в которых можно указать любое соотношение ресурсов.

После создания облачного сервера можно изменить конфигурацию.

Процессоры

В фиксированных и произвольных конфигурациях различаются доступные процессоры. Посмотреть доступные процессоры для разных линеек и пулов можно в таблице Процессоры.

Фиксированные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные серверы.

Фиксированную конфигурацию можно выбрать при создании облачного сервера в панели управления. Если вы создаете облачный сервер через OpenStack CLI и Terraform, используйте таблицу Список флейворов фиксированной конфигурации во всех пулах.

В зависимости от линейки в фиксированных конфигурациях доступно до 36 vCPU, 320 ГБ RAM и 1,25 ТБ локального диска.

Standard Line

Линейка фиксированных конфигураций облачных серверов со сбалансированным распределением ресурсов vCPU:RAM в соотношении 1:4 (кроме конфигураций начального уровня и максимальной конфигурации).

Подходит для решения большинства задач, например выполнения кода для веб-сервисов и приложений, размещения интернет-магазинов, создания тестовых сред.

Доступно от 1 до 36 vCPU, от 1 ГБ до 128 ГБ RAM, от 8 ГБ до 1,25 ТБ локального диска.

CPU Line

Линейка фиксированных конфигураций, в которых ресурсы vCPU:RAM сбалансированы в соотношении 1:2.

Подходят для задач перекодирования видео, машинного обучения, обработки данных, построения CI/CD систем и других задач, требующих производительности и скорости вычислений на vCPU.

Доступно от 4 до 24 vCPU, от 8 ГБ до 48 ГБ RAM, от 128 ГБ до 512 ГБ локального диска.

Memory Line

Линейка фиксированных конфигураций, в которых ресурсы vCPU:RAM сбалансированы в соотношении 1:8.

Конфигурации обеспечивают высокую производительность при рабочих нагрузках, связанных с обработкой больших пакетов данных, для размещения требовательных баз данных или корпоративных приложений SAP и 1С.

Доступно от 2 до 16 vCPU, от 16 ГБ до 128 ГБ RAM, от 64 ГБ до 512 ГБ локального диска.

GPU Line

Фиксированные конфигурации облачных серверов с выделенными GPU.

Оптимизированы для вычислений на GPU, например для перекодирования видео, обучения нейросетей или создания удаленных рабочих станций.

Доступно от 4 до 32 vCPU, от 1 до 4 GPU, от 32 ГБ до 320 ГБ RAM.

Линейку GPU Line можно использовать с локальным или сетевым загрузочным диском. Для облачных серверов с локальным диском можно использовать только NVIDIA® A100 или NVIDIA® A30 в сегменте пула ru-7a.

Подробнее в инструкции Создать облачный сервер с GPU.

Shared Line

Фиксированные конфигурации облачных серверов с возможностью использования и оплаты только части vCPU.

Конфигурации Shared Line дешевле других линеек и подходят для задач, которые не требуют постоянной и полной загрузки виртуального ядра, например запуска стейджинга, сайта, поднятия сети или обучения.

В Shared Line одно виртуальное ядро может использоваться сразу несколькими клиентами. При создании такой конфигурации нужно указать долю vCPU, которая зарезервируется за вашим сервером: 10%, 20% или 50%. Производительность облачного сервера никогда не опустится ниже указанной доли и может временно доходить до 100%,

если другие клиенты используют ресурсы не по максимуму или часть виртуального ядра не арендована.

Используются только с сетевым загрузочным диском.

Доступно от 1 до 4 vCPU, от 512 МБ до 8 ГБ RAM.

HighFreq Line

Фиксированные конфигурации высокопроизводительных облачных серверов с частотой процессора до 3,6 ГГц, памяти — 3 200 МГц.

Подходят для баз данных, например 1С Bitrix, игровых серверов и других задач, требующих высокой скорости обработки и отклика.

Используются только с локальным загрузочным диском — это помогает избежать сетевых задержек.

Доступно от 1 до 8 vCPU, от 2 ГБ до 64 ГБ RAM, от 30 ГБ до 960 ГБ локального диска.

SGX Line

Фиксированные конфигурации облачных серверов, поддерживающих технологию SGX. Технология позволяет приложению создавать в оперативной памяти защищенные области.

Подходят для хранения и обработки конфиденциальных данных, в том числе персональной и платежной информации.

Доступно от 1 до 24 vCPU, от 4 ГБ до 96 ГБ RAM, от 2 ГБ до 64 ГБ EPC, от 32 ГБ до 1 ТБ локального диска.

Подробнее в инструкции Создать облачный сервер SGX.

Произвольные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные серверы.

Произвольную конфигурацию можно выбрать при создании облачного сервера в панели управления. Если вы создаете облачный сервер через OpenStack CLI и Terraform и фиксированные конфигурации не подходят, создайте флейвор. Флейворы определяют количество vCPU, RAM и размер локального диска (опционально) сервера. Через OpenStack API можно создать флейвор с GPU.

Значения произвольных конфигураций

В произвольных конфигурациях можно выбрать любое соотношение ресурсов и добавить GPU. Доступные значения зависят от сегмента пула.

Если произвольные конфигурации не подходят, вы можете заказать собственную конфигурацию. Создайте тикет и укажите соотношение ресурсов:

- vCPU:RAM — не менее 1:2;
- vCPU:RAM:Локальный диск — не менее 1:2:16.

Создать облачный сервер

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. Нажмите **Создать сервер**.
3. В блоке **Имя и расположение**:
   3.1. В поле **Имя** введите имя сервера. Оно будет установлено как имя хоста в операционной системе.
   3.2. В полях **Регион** и **Пул** выберите регион и сегмент пула, в котором будет создан сервер. От сегмента пула зависит список доступных конфигураций сервера и стоимость ресурсов. После создания сервера изменить сегмент пула нельзя.
4. В блоке **Источник** нажмите на имя источника по умолчанию и выберите источник, из которого будет создан сервер:
   4.1. Чтобы создать сервер из готового образа с предустановленной и настроенной операционной системой, откройте вкладку **Готовые образы**, выберите образ и нажмите **Выбрать**. Готовые образы доступны во всех сегментах пула.
   4.2. Чтобы создать сервер с приложением, откройте вкладку **Приложения**, выберите приложение и нажмите **Выбрать**. Приложения доступны во всех сегментах пула.
   4.3. Чтобы создать сервер из собственного образа, который вы самостоятельно загрузили в хранилище образов, откройте вкладку **Мои образы**, выберите образ и нажмите **Выбрать**. Образ должен находиться в одном сегменте пула с сервером.
   4.4. Чтобы создать сервер из созданного сетевого диска, откройте вкладку **Диски**, выберите диск и нажмите **Выбрать**. Диск должен находиться в одном сегменте пула с сервером.
   4.5. Чтобы создать сервер из снапшота сетевого диска, откройте вкладку **Снапшоты**, выберите снапшот и нажмите **Выбрать**. Снапшот должен находиться в одном сегменте пула с сервером.
5. В блоке **Конфигурация** выберите конфигурацию сервера:
   - фиксированную конфигурацию — линейки, в которых зафиксировано соотношение ресурсов;
   - или произвольную конфигурацию, в которой можно указать любое соотношение ресурсов.

   В конфигурациях используются разные процессоры в зависимости от линейки и сегмента пула.
   5.1. Чтобы выбрать фиксированную конфигурацию, нажмите **Фиксированная**, откройте вкладку с нужной линейкой и выберите конфигурацию.
   5.2. Чтобы выбрать произвольную конфигурацию, нажмите **Произвольная**, укажите количество vCPU и размер RAM. Если нужно добавить к серверу графические процессоры, нажмите **Добавить GPU**, выберите тип GPU и укажите количество GPU.
   5.3. Чтобы в качестве загрузочного диска сервера выбрать локальный диск,

отметьте чекбокс **Локальный SSD NVMe диск**. Сервер с локальным диском можно создать только из образов и приложений. Чтобы в качестве загрузочного диска выбрать сетевой диск, не отмечайте чекбокс.

Объем оперативной памяти, который выделяется серверу, может быть меньше указанного в конфигурации — ядро операционной системы резервирует часть оперативной памяти в зависимости от версии ядра и дистрибутива. Выделенный объем на сервере можно проверить с помощью команды `sudo dmesg | grep Memory`.

После создания сервера можно изменить конфигурацию.

6. Если вы не отметили чекбокс **Локальный SSD NVMe диск** на шаге 5.3., в качестве загрузочного диска сервера будет использоваться первый указанный сетевой диск. В блоке **Диски**:

   6.1. В поле **Тип диска** выберите тип сетевого загрузочного диска.

   6.2. Укажите размер сетевого загрузочного диска в ГБ или ТБ. Учитывайте лимиты сетевых дисков на максимальный размер.

   6.3. Если вы выбрали тип диска Универсальный v2, укажите количество IOPS. После создания диска вы можете изменить количество IOPS — уменьшить или увеличить. Количество изменений IOPS неограниченно.

7. Опционально: добавьте дополнительные сетевые диски сервера. В блоке **Диски**:

   7.1. В поле **Тип диска** выберите тип сетевого диска.

   7.2. Укажите размер сетевого диска в ГБ или ТБ. Учитывайте лимиты сетевых дисков на максимальный размер.

   7.3. Если вы выбрали тип диска Универсальный v2, укажите количество IOPS. После создания диска вы можете изменить количество IOPS — уменьшить или увеличить. Количество изменений IOPS неограниченно.

   7.4. Чтобы добавить другой дополнительный диск, нажмите **Добавить**, выберите тип диска и укажите его размер.

   После создания сервера можно отключить от него дополнительные диски или подключить новые.

8. В блоке **Сеть** выберите подсеть, к которой будет подключен сервер:
   - приватная — подсеть без доступа из интернета;
   - приватная + 1 публичный IP — приватная подсеть со статическим публичным IP-адресом. По умолчанию в подсети из интернета будет доступен только сервер, к которому подключается публичный IP-адрес;
   - публичная — подсеть, в которой все адреса доступны из интернета.

   8.1. Чтобы создать приватную подсеть без доступа из интернета, в поле **Подсеть** выберите **Приватная**. Опционально: измените сетевые настройки по умолчанию, для этого в поле **CIDR подсети** укажите CIDR подсети, включите или выключите тумблер **DHCP**, в поле **Шлюз** укажите IP-адрес шлюза по умолчанию, в поле **Подсеть будет создана в сети** выберите **Новая сеть** и введите имя сети.

   Если приватная подсеть создана, в поле **Подсеть** выберите существующую

подсеть и в поле **Приватный IP** укажите приватный IP-адрес сервера.
8.2. Чтобы создать приватную подсеть и статический публичный IP-адрес, в поле **Подсеть** выберите **Приватная + 1 публичный IP**. Автоматически будут созданы приватная сеть `nat`, приватная подсеть, роутер `router-nat` и публичный IP-адрес.
Если приватная подсеть и облачный роутер, подключенный к внешней сети, созданы, в поле **Подсеть** выберите **Приватная + 1 публичный IP**, в поле **Приватная подсеть** выберите созданную подсеть, в поле **Приватный IP** укажите приватный IP-адрес сервера. Если публичный IP-адрес создан, нажмите **Подключить существующий** и выберите публичный IP-адрес.
8.3. Чтобы создать публичную подсеть, в поле **Подсеть** выберите **Публичная** и в поле **Размер подсети** выберите количество IP-адресов в подсети.
Если публичная подсеть создана, в поле **Подсеть** выберите существующую подсеть и в поле **Публичный IP** укажите публичный IP-адрес сервера.

9. В блоке **Доступ**:
   9.1. Разместите на сервере SSH-ключ для проекта для безопасного подключения.
   Чтобы добавить в облачную платформу новый SSH-ключ для проекта, нажмите **Добавить SSH-ключ**, введите имя ключа, вставьте публичный SSH-ключ в формате OpenSSH и нажмите **Добавить**.
   Если SSH-ключ добавлен в облачную платформу, в поле **SSH-ключ** выберите существующий ключ.
   SSH-ключ доступен только в том пуле, в котором он размещен.
   9.2. Опционально: в поле **Пароль для «root»** скопируйте пароль пользователя `root` (пользователь с неограниченными правами на все действия над системой). Сохраните пароль в безопасном месте и не передавайте в открытом виде.
10. В блоке **Дополнительные настройки**:
    10.1. Опционально: чтобы создать прерываемый сервер, отметьте чекбокс **Прерываемый сервер**.
    10.2. Опционально: если вы планируете создать несколько серверов и хотите повысить отказоустойчивость инфраструктуры, добавьте сервер в группу размещения. Чтобы создать новую группу, нажмите **Создать группу**, введите имя группы и выберите политику размещения на разных хостах:
    - желательно — soft-anti-affinity. Система постарается разместить серверы на разных хостах. Если при создании сервера не будет подходящего хоста, он будет создан на том же хосте;
    - обязательно — anti-affinity. Серверы в группе обязательно располагаются на разных хостах. Если при создании сервера не будет подходящего хоста, сервер не будет создан.

    Если группа создана, в поле **Группа размещения** выберите группу размещения.
    10.3. Опционально: добавьте теги сервера, чтобы добавить дополнительную информацию или фильтровать серверы в списке. Автоматически добавляются теги операционной системы и конфигурации. Чтобы добавить новый тег, в поле **Теги** введите тег.

11. Опционально: в блоке **Автоматизация** в поле **User data** вставьте скрипт, который выполнится с помощью агента cloud-init при первом запуске операционной

системы. Откройте вкладку **Текст** и вставьте скрипт или откройте вкладку **Файл** и загрузите файл. Примеры скриптов и поддерживаемые форматы можно посмотреть в инструкции User data.
12. Проверьте цену облачного сервера.
13. Нажмите **Создать**.

Создать прерываемый облачный сервер

Прерываемый облачный сервер — это облачный сервер, который работает не более 24 часов после создания и может быть остановлен со стороны Selectel в любой момент, например, если на виртуальном хосте не хватит ресурсов для других облачных серверов.

При системном прерывании облачный сервер не удаляется — он останавливается и переходит в статус `EXPIRED`. После прерывания сервер можно восстановить. На сервере с сетевым загрузочным диском сохраняются все данные, с локальным — удаляются. Подробнее о восстановлении прерываемого сервера.

Прерываемые серверы поддерживают все функции, которые доступны для обычных облачных серверов, при этом их стоимость ниже в среднем на 70%.

Можно сделать облачный сервер прерываемым при создании сервера или после — изменить тип сервера. Прерываемым можно сделать сервер любой конфигурации.

Для каких задач подходит

Подходит для fault-tolerant систем, в которых используется несколько серверов и при выходе из строя некоторых из них нагрузка перераспределяется на другие серверы:

- для параллельной пакетной обработки данных;
- тестирования CI/CD;
- проектов Hadoop и Kubernetes;
- масштабирования отказоустойчивых веб-сервисов в пиковые моменты нагрузки;
- любых отказоустойчивых проектов с переменной нагрузкой.

Ограничения

Прерываемые облачные серверы временно доступны только в пуле ru-7.

Мы не гарантируем уровень доступности как у обычных облачных серверов — на прерываемые серверы не действует SLA для облачной платформы.

Стоимость

Стоимость прерываемого сервера ниже в среднем на 70%, чем стоимость обычного облачного сервера с такой же конфигурацией.

Во время работы прерываемые облачные серверы оплачиваются по модели оплаты облачной платформы.

После прерывания:

- за vCPU, RAM, GPU, локальные диски средства перестают списываться, начиная со следующего часа после остановки;
- за публичные IP-адреса, публичные подсети и сетевые диски средства продолжают списываться.

Создать прерываемый сервер

Прерываемый сервер будет остановлен со стороны Selectel в любой момент в течение 24 часов после создания.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. Нажмите **Создать сервер**.
3. В блоке **Дополнительные настройки** отметьте чекбокс **Прерываемый сервер**.
4. Выберите остальные настройки сервера — подробнее в инструкции Создать облачный сервер.
5. Нажмите **Создать**.

Изменить тип сервера

Можно изменить тип облачного сервера — сделать непрерываемый сервер прерываемым и наоборот.

Прерываемый сервер будет остановлен со стороны Selectel в любой момент в течение 24 часов после создания. После каждого изменения типа сервера на прерываемый отсчет 24 часов начинается заново.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. Откройте страницу сервера → вкладка **Конфигурация**.
3. В блоке **Тип сервера** нажмите .
4. Проверьте новую стоимость сервера и нажмите **Изменить**.

Восстановить прерываемый сервер

Можно восстановить прерываемый сервер в статусе `EXPIRED` — возобновить его работу.

Восстановление зависит от типа загрузочного диска:

- если диск сетевой, сервер восстанавливается из диска и продолжает работу в состоянии, в котором был на момент остановки;
- если диск локальный, создается новый облачный сервер из образа, из которого он был создан. Данные, которые появились на сервере в процессе работы, не восстанавливаются.

После восстановления сервер продолжит быть прерываемым и будет остановлен со стороны Selectel в любой момент в течение 24 часов после восстановления.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. В меню ⋮ сервера выберите **Возобновить**.

Работа с облачным сервером

Изменить конфигурацию облачного сервера

У облачного сервера можно изменить конфигурацию и количество ресурсов:

- выбрать другую линейку фиксированной конфигурации (кроме линейки GPU Line);
- изменить фиксированную конфигурацию на произвольную (кроме линеек SGX Line и GPU Line);
- изменить произвольную на фиксированную;
- изменить количество ресурсов в текущей фиксированной или произвольной конфигурации — vCPU, RAM, объема локального диска.

Конфигурацию облачного сервера с локальным диском нельзя изменить на конфигурацию без локального диска и наоборот.

При изменении конфигурации все данные на облачном сервере сохраняются.

К серверам произвольной конфигурации можно добавить графические процессоры.

Изменить конфигурацию сервера

Во время изменения конфигурации облачный сервер будет недоступен.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. Откройте страницу сервера → вкладка **Конфигурация**.
3. Нажмите **Изменить конфигурацию**.
4. В блоке **Конфигурация** выберите новую конфигурацию: фиксированную или произвольную.
5. Укажите нужное количество ресурсов.
6. Нажмите **Сохранить и перезагрузить**.

Управлять работой облачного сервера

Вы можете управлять работой облачного сервера: выключить и включить, заморозить и возобновить работу после заморозки, приостановить и возобновить работу после паузы.

Если облачный сервер выключен или приостановлен, продолжают оплачиваться все ресурсы облачной платформы: vCPU, RAM, локальные и сетевые диски, GPU, публичные IP-адреса, публичные подсети. Если сервер заморожен, не тарифицируются vCPU, RAM и GPU, при этом все остальные ресурсы оплачиваются. Подробнее о модели оплаты облачной платформы.

Выключить сервер

При выключении сервера операционная система корректно завершит работу, будет выключено питание.

Если сервер не ответит в течение фиксированного времени, то он будет остановлен принудительно — в таком случае могут быть потеряны несохраненные данные.

Если облачный сервер выключен, продолжают оплачиваться все ресурсы облачной платформы: vCPU, RAM, локальные и сетевые диски, GPU, публичные IP-адреса, публичные подсети. Подробнее о модели оплаты облачной платформы.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. В меню ⁞ сервера выберите **Выключить**. Сервер перейдет в статус `SHUTOFF`.

Включить сервер

Если сервер был выключен, при включении заново начнется загрузка операционной системы, подключение дисков и портов.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. В меню ⁞ сервера выберите **Включить**. Сервер перейдет в статус `ACTIVE`.

Заморозить сервер

Заморозка — это выключение облачного сервера, при котором vCPU, RAM и GPU передаются в общий пул ресурсов и перестают тарифицироваться. При этом продолжают оплачиваться другие ресурсы облачной платформы: сетевые диски, публичные IP-адреса, публичные подсети. Подробнее о модели оплаты облачной платформы.

Можно заморозить облачные серверы только с загрузочным сетевым диском. Серверы с локальным диском заморозить нельзя.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. В меню ⁞ сервера выберите **Заморозить**. Сервер перейдет в статус `FROZEN`.

Возобновить работу сервера после заморозки

При возобновлении работы сервера создается облачный сервер с тем же количеством vCPU, RAM и GPU, которое было на момент заморозки. Сервер создается при наличии ресурсов в общем пуле.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. В меню ⁞ сервера выберите **Возобновить**. Сервер перейдет в статус `ACTIVE`.

Перезагрузить облачный сервер

Вы можете перезагрузить облачный сервер — программно или аппаратно (через отключение питания).

Выполнить программную перезагрузку

Сервер перезагрузится без отключения питания. Выполнится graceful shutdown — операционная система корректно завершит работу и запустится заново.

Если сервер не ответит в течение фиксированного времени, то он будет принудительно перезагружен аппаратно — в таком случае могут быть потеряны несохраненные данные.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. В меню ⁞ сервера выберите **Программная перезагрузка**.

Выполнить аппаратную перезагрузку

При аппаратной перезагрузке сервер выключается и сразу же включается — при этом не происходит пересоздание конфигурации.

Мы рекомендуем выполнять аппаратную перезагрузку, только если сервер не отвечает — в остальных случаях выключите и включите сервер.

1. В панели управления перейдите в раздел **Облачная платформа → Серверы**.
2. В меню ⋮ сервера выберите **Перезагрузка по питанию**.

Посмотреть статус облачного сервера

1. В панели управления перейдите в раздел **Облачная платформа → Серверы**.
2. Откройте вкладку **Серверы**.
3. Посмотрите статус в строке сервера.

ACTIVE	Сервер включен и работает
PAUSED	Сервер приостановлен (пауза)
FROZEN **(в OpenStack CLI — SHELVED_OFFLOADED)**	Сервер заморожен
EXPIRED **(в OpenStack CLI — SHELVED_OFFLOADED)**	Прерываемый сервер остановлен
SHUTOFF	Сервер выключен
REBOOT_STARTED	Сервер перезагружается программно
REBOOT_STARTED_HARD	Сервер перезагружается аппаратно
REBUILDING	Сервер пересоздается
RESCUE	Сервер загружен в режим восстановления и диагностики Rescue

ERROR	Произошла ошибка в работе сервера. Пересоздайте сервер
DELETING	Сервер удаляется
DELETED	Сервер удален

User data

User data — пользовательские параметры конфигурации операционной системы сервера. Описываются в виде скриптов в формате cloud-config (текстовые файлы с YAML-синтаксисом) или как bash-скрипт. Скрипты автоматически кодируются в Base64, передаются на сервер и выполняются с помощью агента cloud-init при первом запуске операционной системы. Использование user data помогает автоматизировать настройку серверов.

Указать user data можно при создании облачного сервера.

Подробнее о форматах скриптов cloud-config и bash в инструкции User data formats документации cloud-init.

В скриптах можно передавать параметры для настройки операционной системы и сценарии. Например:

- создать каталог и загрузить в него файлы;
- обновить репозитории и установить пакеты программного обеспечения;
- разместить SSH-ключи на сервере;
- настроить файл конфигурации преобразователя доменных имен resolv.conf.

Посмотрите другие примеры в инструкции Cloud config examples документации cloud-init.

Указать user data

Указать user data можно только при создании облачного сервера:

- в панели управления — на шаге 14 можно вставить текст в поле **User data**, загрузить файл в форматах `txt`, `gz`, `sh` или MIME-архив. Максимальный размер скрипта с данными, которые не закодированы в Base64, — 16 КБ;
- через OpenStack CLI и Terraform — только скрипты с данными, закодированными в Base64.

После создания сервера изменить скрипт нельзя.

Посмотреть статистику использования ресурсов облачного сервера

Вы можете посмотреть информацию о нагрузке на облачные серверы в виде графиков.

Если облачный сервер выключен, метрики не собираются.

Сбор значений для всех метрик происходит раз в 5 минут. Если вы только что создали сервер, первые значения метрик сетевых интерфейсов и дисков появятся через 10 минут.

Посмотреть статистику использования ресурсов

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. Откройте страницу сервера → вкладка **Статистика**.
3. Посмотрите доступные метрики облачного сервера.

Метрики облачного сервера в панели управления

CPU	На сколько процентов загружены vCPU облачного сервера
Память	Занятая оперативная память без учета кеша и буферов операционной системы в гигабайтах
Диск	Нагрузка на диск (чтение и запись) в байтах или количестве операций в секунду
Сеть	Входящий и исходящий трафик в битах или пакетах в секунду

Удалить облачный сервер

Локальный загрузочный диск удаляется вместе с сервером, сетевой загрузочный диск можно отключить от сервера перед удалением.

При удалении сервера загрузочные диски и дополнительные диски, если вы выбрали их удаление, уничтожаются встроенными средствами облачной платформы. Программно-определяемое хранилище разбивает информацию на большое количество блоков и хранит их на разных физических дисках — это не позволяет восстановить информацию при получении физического доступа к одному из дисков. Если физический диск вышел из строя, он подключается к служебному оборудованию. Если диск определяется, производится полная затирка программными средствами, если не определяется — выводится из эксплуатации и уничтожается.

После удаления облачный сервер и его диски нельзя восстановить.

1. Опционально: чтобы сохранить данные, отключите от сервера сетевой загрузочный диск.
2. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
3. В меню ⋮ сервера выберите **Удалить сервер**.
4. Опционально: для удаления всех дисков отметьте чекбокс **Удалить диски этого сервера**.
5. Нажмите **Удалить**.

Группы размещения

Группы размещения

Облачный сервер можно добавить в группу размещения. Серверы в группе могут располагаться на разных физических хостах — это повышает отказоустойчивость инфраструктуры.

Группа размещения создается для определенного пула. При этом облачные серверы в группе могут находиться в разных сегментах внутри пула.

Работать с группами размещения можно работать в панели управления, с помощью OpenStack CLI или Terraform.

Политика размещения

При создании группы можно выбрать политику группы — она определяет, как серверы будут располагаться на физическом оборудовании:

- желательно на разных хостах (soft-anti-affinity) — система будет стремиться разместить серверы на разных хостах. Если при создании сервера не будет подходящего хоста, он будет создан на том же хосте;
- обязательно на разных хостах (anti-affinity) — серверы в группе обязательно располагаются на разных хостах. Если мы не найдем подходящий хост, сервер не будет создан.

Ограничения

Группу можно создать только для одного пула.

В одном проекте можно создать не более 100 групп размещения.

В одной группе одновременно может находиться не более 15 облачных серверов.

Добавить облачный сервер в группу размещения можно только при создании облачного сервера.

Стоимость

Создание группы размещения бесплатно.

Оплачиваются только облачные серверы, входящие в группу, и другие ресурсы облачной платформы — по модели оплаты облачной платформы.

Создать группу размещения

Группу размещения можно создать:

- при создании облачного сервера — созданный сервер автоматически добавится в группу;
- или отдельно — облачный сервер можно будет добавить в эту группу только при создании сервера.

1. В панели управления перейдите в раздел **Облачная платформа → Серверы**.
2. Откройте вкладку **Группы размещения**.
3. Нажмите **Создать группу**.
4. Введите имя группы.
5. Выберите политику размещения:
    - желательно на разных хостах (soft-anti-affinity) — система будет стремиться разместить серверы на разных хостах. Если при создании сервера не будет подходящего хоста, он будет создан на том же хосте;
    - обязательно на разных хостах (anti-affinity) — серверы в группе обязательно располагаются на разных хостах. Если мы не найдем подходящий хост, сервер не будет создан.
6. Нажмите **Создать группу**.

Добавить облачный сервер в группу размещения

Добавить облачный сервер в группу размещения можно только при создании облачного сервера.

Существующий сервер нельзя напрямую добавить в группу размещения, но можно при создании копии сервера добавить его в группу.

Добавить облачный сервер в группу при создании сервера

Используйте инструкцию Создать облачный сервер.

Добавить существующий облачный сервер в группу

Существующий облачный сервер нельзя добавить в группу. Создайте копию облачного сервера и при создании добавьте сервер в группу размещения.

1. Если у облачного сервера локальный загрузочный диск, создайте образ из диска.
2. Если у облачного сервера сетевой загрузочный диск, выберите один из вариантов:
    - создайте образ из диска;
    - создайте снапшот диска;
    - или отключите загрузочный диск от облачного сервера.
3. Используйте инструкцию Создать облачный сервер. В качестве источника выберите созданный образ, снапшот или диск, который отключили от сервера.

Исключить облачный сервер из группы размещения

При исключении из группы размещения облачный сервер не будет удален и не изменит расположение — он останется на прежнем хосте.
Сервер может мигрировать на другой хост при изменении конфигурации сервера или оптимизации инфраструктуры со стороны Selectel.

1. В панели управления перейдите в раздел **Облачная платформа → Серверы**.
2. Откройте вкладку **Группы размещения**.
3. Откройте карточку группы.
4. В строке с облачным сервером нажмите 🗑️.
5. Введите имя сервера для подтверждения удаления.
6. Нажмите **Удалить**.

Удалить группу размещения

При удалении группы размещения облачные серверы не будут удалены и не изменят расположение — они останутся на прежних хостах.

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. Откройте вкладку **Группы размещения**.
3. В карточке группы нажмите 🗑️.

Диски

Локальные диски

Локальный диск подключается напрямую к серверу вычислений через интерфейс PCIe по NVMe-протоколу. Поэтому локальный диск можно создать только с облачным сервером и использовать как загрузочный (системный) диск.

У локального диска отсутствуют сетевые задержки, поэтому он подходит для задач, чувствительных к показателям скорости чтения и записи.

Особенности локального диска

- SSD NVMe-диск.
- Производительность — чтение 12800 IOPS, запись 6400 IOPS.
- Пропускная способность — 300 МБ/с.
- Рекомендуемый максимальный объем диска — 2 ТБ.
- Дисковая подсистема сконфигурирована в RAID 10.
- Может быть только загрузочным диском облачного сервера, не используется в качестве дополнительного. Как дополнительные можно подключать только сетевые диски.
- У облачного сервера может быть только один локальный диск.
- Нельзя отключить от облачного сервера и подключить к другому серверу.
- Нельзя увеличить напрямую, можно только изменить конфигурацию облачного сервера.
- Из локального диска нельзя создать другой диск, снапшот или бэкап. Можно создать образ диска (например, для быстрого клонирования сервера).
- Удаляется со всеми данными при удалении облачного сервера.

Стоимость

Локальные диски оплачиваются по модели оплаты облачной платформы.

Стоимость локального диска зависит от его размера и сегмента пула, в котором создается облачный сервер с этим диском.

Оплачивается каждый ГБ локальных дисков. Стоимость одного ГБ можно посмотреть на selectel.ru.

Сетевые диски

Сетевые диски — это масштабируемые блочные устройства, которые можно легко переносить между облачными серверами. Подходят для масштабирования дискового пространства сервера без изменения загрузочного диска. Трехкратная репликация томов диска обеспечивает высокую сохранность данных.

Сетевой диск можно создать вместе с облачным сервером или создать отдельно, а затем создать из него сервер или подключить к серверу как дополнительный диск.

С сетевыми дисками можно работать в панели управления, с помощью OpenStack CLI или Terraform.

Особенности сетевых дисков

- доступно пять типов сетевых дисков с разными рекомендуемыми ограничениями на размер, значениями пропускной способности и лимитами IOPS;
- можно использовать как загрузочный (системный) диск облачного сервера или подключить как дополнительный диск;
- к одному облачному серверу можно подключить до 255 сетевых дисков, если вы используете стандартный диск со свойством virtio-scsi (при использовании ide — до 4, при использовании virtio-blk — до 26);
- сетевой диск можно отключить от сервера;
- можно увеличить сетевой диск;
- из сетевого диска можно создать образ, снапшот или другой диск, настроить бэкапы;
- можно переносить диск между сегментами пула, проектами и аккаунтами.

Типы сетевых дисков

- HDD Базовый — HDD-диск на базе SATA-дисков enterprise-класса. Подходит для хранения больших объемов данных, которые не нужно часто читать или перезаписывать;
- SSD Базовый — SSD-диск для задач, в которых не требуется высокая скорость чтения и записи. Пропускная способность и IOPS выше, чем у базового HDD;
- SSD Универсальный — SSD-диск, подходит для использования в качестве загрузочного диска облачного сервера;
- SSD Универсальный v2 — SSD-диск с возможностью изменения лимита IOPS и без фиксированного разделения количества операций на чтение и запись. Подходит для задач с неравномерной нагрузкой. При выборе максимального количества IOPS подходит для CRM систем, систем мониторинга и для работы с большими данными;
- SSD Быстрый — SSD NVMe-диск с меньшим временем отклика и большей скоростью работы по сравнению с другими типами. Подходит для нагрузок, которые требуют высокой скорости чтения и записи.

Типы дисков отличаются рекомендуемыми ограничениями на размер, значениями пропускной способности и количеством операций на чтение и запись. Подробнее в таблице Лимиты сетевых дисков.

В разных сегментах пула доступны разные типы дисков. Посмотреть доступность типов можно в матрице доступности Сетевые диски облачной платформы.

Посмотреть список ID и имен типов можно в подразделе Список типов сетевого диска.

Лимиты сетевых дисков

Максимальный размер загрузочных и дополнительных сетевых дисков, значения пропускной способности и лимиты на чтение и запись в IOPS зависят от типа диска.

Диски одного типа в разных сегментах пула могут иметь разные лимиты. Например, если два сетевых диска с типом SSD Универсальный находятся в разных сегментах (первый диск в ru-1c, второй — в ru-8a), их лимиты будут различаться. Вы можете протестировать производительность дисков.

Что влияет на производительность

Разные типы дисков имеют разные значения IOPS — число операций чтения и записи в секунду. Создание и проверка файловой системы — это процедуры, которые требуют выполнения определенного количества операций чтения и записи на диск. Чем производительнее диск, тем быстрее завершаются данные операции.

При первом запуске облачного сервера файловая система на системном диске «растягивается» по размеру диска. Чем больше размер диска и чем ниже у него лимиты на IOPS, тем дольше будет длиться этот процесс — следовательно, дольше будет запускаться облачный сервер.

Размер файловой системы влияет на время проверки ее состояния в случае аварийного завершения работы сервера. Проверка включена по умолчанию для загрузочных (системных) дисков всех серверов, которые создаются из готовых образов.

Стоимость

Сетевые диски оплачиваются по модели оплаты облачной платформы.

Оплачивается каждый ГБ сетевых дисков. Стоимость зависит от типа сетевого диска, размера и сегмента пула, в котором он расположен.

Размер сетевого диска можно посмотреть в панели управления в разделе **Облачная платформа** → **Диски** → строка диска → столбец **Размер**.

Для сетевых дисков типа SSD Универсальный v2 также оплачивается количество используемых IOPS. Учитывается максимальное количество IOPS в час. Первые 2 000 IOPS предоставляются бесплатно. Количество IOPS можно посмотреть в панели управления в разделе **Облачная платформа** → **Диски** → страница диска → вкладка **Настройки**.

Стоимость одного ГБ (для всех типов сетевого диска) и одного IOPS (для дисков типа SSD Универсальный v2) можно посмотреть на selectel.ru.

Создать диск

Сетевой диск можно создать вместе с облачным сервером или создать отдельно, а затем подключить к серверу.

Локальный диск создается только вместе с облачным сервером.

Сетевой диск можно создать из разных источников:

- пустой — изначально такой диск не содержит данные. Вы можете использовать его для масштабирования дискового пространства на облачном сервере;
- из образа — подготовленного Selectel или вашего собственного загруженного образа. Можно использовать для замены загрузочного диска при восстановлении сервера или для клонирования сервера;
- из другого диска, снапшота или бэкапа — создать копию диска.

Стоимость сетевого диска зависит от типа диска и сегмента пула, в котором он создается. Рассчитать стоимость можно в калькуляторе ресурсов.

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. Нажмите **Создать диск**.
3. Введите новое имя диска или оставьте имя, которое создано автоматически.

4. Выберите расположение диска — пул и сегмент пула. Это должен быть сегмент пула облачного сервера, к которому вы в дальнейшем подключите диск. Сегмент пула влияет на стоимость и лимиты диска.
5. Выберите источник диска (готовый образ, собственный образ, диск, снапшот или бэкап) и нажмите **Выбрать**. Если вы хотите создать пустой диск, пропустите этот шаг.
6. Выберите тип диска. Диски отличаются скоростью чтения/записи и значениями пропускной способности.
7. Укажите размер диска в ГБ. Размер диска, созданного из источника, должен быть равен или больше размера источника. Мы рекомендуем не превышать ограничения дисков на максимальный размер. После создания диск нельзя будет уменьшить напрямую.
8. Если вы выбрали тип диска Универсальный v2, укажите количество IOPS. После создания диска вы можете изменить количество IOPS — уменьшить или увеличить. Количество изменений IOPS неограниченно.
9. Настройте создание бэкапов по расписанию для диска. Выберите ранее созданный план или создайте новый.
10. Нажмите **Создать диск**.

Изменить параметры диска

Изменить тип диска

Изменить тип можно только у сетевого диска — на другой сетевой или на локальный.

Изменить диск на другой сетевой диск

Изменить тип сетевого диска на другой напрямую невозможно — нужно создать новый диск с нужным типом.

1. В сегменте пула текущего диска:
   - создайте образ диска;
   - или отключите текущий диск от облачного сервера и создайте из него новый диск.
2. Опционально: подключите созданный диск к серверу и отключите предыдущий.
3. Опционально: если вы подключили диск как загрузочный (системный), то перезагрузите сервер.

Изменить диск на другой локальный диск

Изменить тип сетевого диска на локальный напрямую невозможно — создайте новый облачный сервер с локальным диском.

1. В сегменте пула текущего диска:
   - создайте образ диска;
   - или отключите текущий диск от облачного сервера и создайте из него новый диск.

2. Создайте новый облачный сервер с локальным диском и выберите в качестве источника созданный образ или диск.

Уменьшить диск

Локальный диск уменьшить невозможно.
Уменьшить размер сетевого диска напрямую нельзя, так как это может нарушить целостность файловой системы диска и данных — можно создать новый диск меньшего объема.

1. В сегменте пула текущего диска создайте пустой диск меньшего объема.
2. Подключите созданный диск к облачному серверу.
3. Загрузите сервер в режим Rescue.
4. Перенесите данные со старого диска на новый — скопируйте файлы вручную или используйте утилиту `dd`.
5. Опционально: отключите старый диск от сервера и удалите диск.

Увеличить диск

Увеличить локальный диск напрямую нельзя — можно изменить конфигурацию облачного сервера, к которому он подключен. Локальный диск расширится автоматически.
Увеличить сетевой диск можно по инструкциям ниже. После увеличения необходимо подготовить диск к работе.
Другой способ увеличения дискового пространства на облачном сервере — подключение дополнительного диска.
Перед выполнением работ с разделами и файловой системой мы рекомендуем создать образ диска, снапшот или другой диск из этого диска, чтобы избежать потери данных в случае ошибки.

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. В меню ⋮ диска выберите **Изменить размер**.
3. Укажите новое значение размера диска в ГБ, учитывайте ограничения дисков на максимальный размер. Нажмите **Сохранить**.
4. Подготовьте диск к работе:
   - если вы увеличили загрузочный диск, перезагрузите облачный сервер или расширьте диск по инструкции;
   - если вы увеличили дополнительный диск, то расширьте диск по инструкции.

Изменить количество IOPS

Изменить количество IOPS можно только у сетевого диска типа SSD Универсальный v2 в статусах `AVAILABLE` и `IN-USE`. Количество изменений IOPS неограниченно.

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. Откройте страницу диска → вкладка **Настройки**.
3. В поле **IOPS** нажмите .
4. Измените количество IOPS.
5. Нажмите **Подтвердить изменения**.

Отключить сетевой диск от сервера

Отключить от облачного сервера можно только сетевой диск — загрузочный или дополнительный.

1. Если диск загрузочный, выключите облачный сервер.
2. Если диск дополнительный, мы также рекомендуем выключить сервер. Вы можете отключить диск и от включенного сервера, но убедитесь, что операционная система полностью загрузилась.
3. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
4. В меню ⁞ диска выберите **Отключить от сервера**.

Перенести диск

Перенести можно только сетевой диск:

- в другой сегмент пула любой зоны доступности и любого региона — при переносе можно выбрать другой проект или аккаунт;
- в другой проект или аккаунт — только внутри одного сегмента пула.

Перенести диск в другой сегмент пула

Чтобы перенести диск в другой сегмент пула, нужно создать его образ, перенести образ и создать из него новый диск. Напрямую перенести диск в другой сегмент пула невозможно.

При переносе образа диска можно выбрать другой проект или аккаунт.

1. Создайте образ диска.
2. Перенесите образ в другой сегмент пула.
3. Создайте диск из образа.

Перенести диск в другой проект или аккаунт

Перенести сетевой диск в другой проект или аккаунт можно только в пределах одного сегмента пула. Можно перенести один диск или несколько сразу.

Перенести один диск

1. Отключите диск от облачного сервера.
2. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
3. В меню ⁞ диска выберите **Перенести в другой проект**.
4. Нажмите **Начать перенос**. Диск перейдет в статус `AWAITING-TRANSFER` и будет недоступен для работы. В открывшемся окне появятся данные для завершения переноса — ID переноса и Ключ.
5. Опционально: чтобы в любой момент отменить перенос (перевести диск обратно в статус `ACTIVE`), в меню ⁞ диска выберите **Управление переносом** и нажмите **Отменить перенос**.
6. В соседней вкладке браузера откройте проект, в который нужно перенести диск.
7. Перейдите в раздел **Облачная платформа** → **Диски**. Убедитесь, что вы открыли список дисков того же сегмента пула, из которого переносится диск.

8. В меню ⋮ заголовка раздела выберите **Принять диски из другого проекта**.
9. В открывшемся окне введите ID переноса и Ключ, которые вы получили на шаге 4. Нажмите **Принять**.

Перенести несколько дисков

1. Отключите диск от облачных серверов.
2. В панели управления перейдите в раздел **Облачная платформа → Диски**.
3. В меню ⋮ заголовка раздела выберите **Перенести диски в другой проект**.
4. Отметьте нужные диски и нажмите **Скачать список**. На ваш компьютер загрузится JSON-файл с данными для переноса. Диски перейдут в статус `AWAITING-TRANSFER` и будут недоступны для работы.
5. Опционально: чтобы в любой момент отменить перенос (перевести диск обратно в статус `ACTIVE`), в меню ⋮ диска выберите **Управление переносом** и нажмите **Отменить перенос**.
6. В соседней вкладке браузера откройте проект, в который нужно перенести диски.
7. Перейдите в раздел **Облачная платформа → Диски**. Убедитесь, что вы открыли список дисков того же сегмента пула, из которого переносятся диски.
8. В меню ⋮ заголовка раздела выберите **Принять диски из другого проекта**.
9. В открывшемся окне откройте вкладку **Несколько дисков**.
10. Нажмите **Загрузить список** и прикрепите JSON-файл, который вы получили на шаге 4. Появится список дисков для переноса.
11. Проверьте список дисков. Нажмите **Принять**.

Снапшоты диска

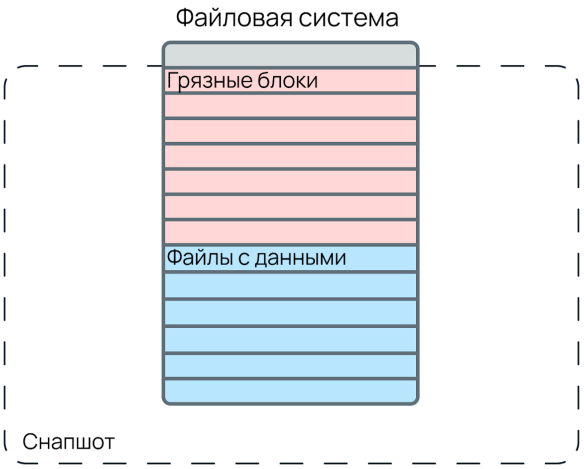
Снапшот — это мгновенный снимок состояния сетевого диска, копия его файловой системы.

С помощью снапшота можно зафиксировать состояние диска, не нарушая его работу, чтобы:

- клонировать диск — для этого можно создать новый диск из снапшота или восстановить данные на новый диск. На диск можно восстановиться сразу после создания снапшота;
- клонировать облачный сервер — создать новый облачный сервер из снапшота;
- изменить тип диска — сохранить состояние диска с помощью снапшота и создать такой же диск, но с другим типом.

Принцип работы

Размер снапшота может превышать реальный объем данных и файлов на диске. В размер снапшота входят блоки файловой системы и «грязные данные», которые появляются при перезаписи или удалении файлов.



Снапшоты можно создать только для сетевых дисков. Для каждого диска можно создать не более пяти снапшотов.

Снапшот не является резервной копией сетевого диска облачного сервера — он хранится на том же оборудовании, требует доступности основного хранилища для выполнения любой операции и удаляется вместе с диском. Если нужно зафиксировать состояние диска и хранить его длительно, вместо снапшота создайте бэкап или создайте образ диска. Если вы хотите настроить автоматическое резервное копирование сетевого диска, настройте создание бэкапов по расписанию.

Снапшот нельзя скачать, но можно создать образ диска и скачать образ.

Посмотреть альтернативные способы создания резервных копий облачных серверов можно в таблице Способы резервного копирования.

Стоимость

Снапшоты оплачиваются по модели оплаты облачной платформы.

Оплачивается каждый ГБ снапшотов со статусами `AVAILABLE` или `RESTORING`. Снапшоты в других статусах не оплачиваются.

Стоимость снапшота равна стоимости сетевого диска, из которого он создан, и зависит от типа диска. Стоимость хранения созданного снапшота не меняется при изменении размера диска.

Оплачивается каждый снапшот диска, даже если снапшотов несколько.

Фактический размер снапшота можно посмотреть в панели управления в разделе **Облачная платформа** → **Диски** → страница диска → вкладка **Снапшоты**. Суммарный объем снапшотов, которые оплачиваются, можно посмотреть в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Текущая стоимость**.

Стоимость одного ГБ снапшотов можно посмотреть на selectel.ru.

Снапшоты, созданные до 2 ноября 2023 года, начнут оплачиваться с 2 ноября. Размер снапшота, который будет оплачиваться, равен размеру диска на момент начала оплаты.

Создать снапшот

Для каждого диска можно создать не более пяти снапшотов. Чтобы увеличить лимит, создайте тикет.

Снапшпот можно создать для сетевых дисков в статусах `AVAILABLE` и `IN-USE`. При создании снапшота имя задается автоматически в виде `snap-датасоздания_времясоздания`, например `snap-14.05.21_14.43`

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. Откройте страницу диска → вкладка **Снапшоты**.
3. Нажмите **Создать снапшот**.

Восстановить данные из снапшота

Вы можете создать новый сетевой диск из снапшота. Диск будет копией состояния, которое было на исходном диске в момент создания снапшота.

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. Откройте страницу диска → вкладка **Снапшоты**.
3. В меню ⋮ снапшота выберите **Создать диск из снапшота**.
4. Опционально: замените загрузочный диск у облачного сервера на восстановленный или подключите к серверу восстановленный диск как дополнительный.

Статусы снапшотов

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. Откройте страницу диска → вкладка **Снапшоты**.
3. Посмотрите статус в строке снапшота → столбец **Статус**.

CREATING	Снапшот создается
AVAILABLE	Снапшот успешно создан, из него можно восстановить данные. Снапшоты в этом статусе оплачиваются
RESTORING	Данные снапшота восстанавливаются на диск. Снапшоты в этом статусе оплачиваются
ERROR	При создании снапшота произошла ошибка
ERROR-DELETING	При удалении снапшота произошла ошибка

DELETING	Снапшот удаляется
DELETED	Снапшот удален

Удалить снапшот

Удалить снапшот можно при удалении диска или отдельно.

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. Откройте страницу диска → вкладка **Снапшоты**.
3. В меню ⁝ снапшота выберите **Удалить**.

Удалить диск

Локальный диск можно удалить только вместе с сервером, к которому он подключен.

Сетевые диски можно удалить вместе с сервером или отключить от сервера и удалить отдельно.

Если вы удалите диск, данные нельзя будет восстановить. Мы рекомендуем сделать копию данных перед удалением диска — создайте образ диска или создайте другой диск из этого диска. Снапшоты диска удалятся вместе с диском.

1. Если диск подключен к облачному серверу, отключите диск от сервера.
2. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
3. В меню ⁝ диска выберите **Удалить диск**.

Файрволы

Облачный файрвол

Облачный файрвол — бесплатный stateful-файрвол. Позволяет настроить сетевую безопасность для приватных подсетей и публичных IP-адресов в облачной платформе.

Работать с облачным файрволом можно в панели управления, с помощью OpenStack CLI или Terraform.

Фильтруемый трафик

С помощью файрвола можно настроить фильтрацию IPv4-трафика для приватной подсети, открыть и закрыть определенные порты или их диапазон, разрешить и запретить доступ с определенных IP-адресов или из подсетей.

Какой трафик фильтруется

Облачный файрвол фильтрует весь IPv4-трафик, проходящий через порт облачного роутера, на который он назначен:

- входящий трафик в приватную подсеть из другой приватной подсети. Приватные подсети должны принадлежать разным приватным сетям:

  Например, приватная подсеть `192.168.0.0/24` находится в приватной сети `network_1`, а приватная подсеть `10.0.0.0/24` находятся в приватной сети `network_2`. Трафик между устройствами в этих подсетях будет фильтроваться.

  Подробнее о приватных сетях и подсетях в инструкции Сети облачной платформы;

- входящий трафик в приватную подсеть из интернета, идущий на публичные IP-адреса устройств (облачных серверов и балансировщиков), которые ассоциированы с их приватным адресом через NAT 1:1;

- исходящий трафик — трафик из приватной подсети в интернет или другую приватную сеть.

Какой трафик не фильтруется

- трафик между устройствами внутри приватной подсети;

- трафик между устройствами из разных приватных подсетей внутри одной приватной сети:

  Например, приватная подсеть `192.168.0.0/24` и приватная подсеть `10.0.0.0/24` находятся в одной приватной сети `network_1`. Трафик между

устройствами в этих подсетях фильтроваться не будет.

- трафик для публичных подсетей. Публичные адреса из таких подсетей назначаются прямо на устройства, и трафик не проходит через порт облачного роутера.

Для фильтрации этих видов трафика используйте утилиты операционной системы, например `iptables`. Подробнее в статье блога Настройка iptables в Linux.

Принцип работы

Облачный файрвол не является отдельным устройством. Он назначается на внутренний порт облачного роутера в приватной подсети, которая подключена к роутеру. Файрвол можно переиспользовать и назначить на несколько портов роутеров одновременно. На один порт роутера нельзя назначить более одного файрвола.

Файрвол по добавленным правилам фильтрации анализирует и фильтрует трафик: входящий, который проходит в приватную подсеть через облачный роутер, и трафик, исходящий из этой подсети. Правила файрвола действуют не на облачный сервер или балансировщик нагрузки, а на IP-адрес. Если вы подключили к устройству другой публичный IP-адрес или пересоздали его с другим публичным IP, нужно изменить IP-адрес в правиле, чтобы трафик продолжил фильтроваться.

В облачном файрволе используется модель OpenStack:

- Firewall Groups (файрволы) — содержат политики. Один файрвол может содержать только одну политику ingress для входящего трафика и одну egress для исходящего трафика;
- Firewall Policies (политики файрвола) — списки правил файрвола в определенном порядке;
- Firewall Rules (правила файрвола) — набор параметров, по которым фильтруется трафик: протоколы, IP-адреса и порты. Правила выполняются в указанном порядке. Подробнее о правилах и параметрах в подразделе Правила.

Подробнее о модели OpenStack в разделе FWaaS документации OpenStack.

Правила

Для облачного файрвола настраиваются две политики (два списка правил в определенном порядке) — для входящего и для исходящего трафика.

Правила выполняются по порядку в списке — сверху вниз. Если первое правило разрешает прохождение трафика, то трафик будет разрешен, даже если в правилах ниже настроен запрет.

Файрвол анализирует трафик на основании параметров в правилах:

- направление трафика (политика) — входящий или исходящий;

- разрешение или запрет трафика;
- протокол — поддерживаются протоколы TCP, UDP, ICMP;
- source — IP-адрес или подсеть источника трафика;
- source port — порт или диапазон портов источника трафика;
- destination — IP-адрес или подсеть назначения трафика;
- destination port — порт или диапазон портов назначения трафика.

У облачного файрвола есть базовое свойство: весь входящий и исходящий трафик, который не разрешен, — запрещен. Например, вы создали файрвол без правил и назначили на порт облачного роутера. Пока вы не добавите разрешающие правила, будут запрещены: трафик, входящий в приватную подсеть, которая подключена к роутеру; трафик, исходящий из этой подсети.

Политики и правила файрвола можно переиспользовать только при работе через OpenStack CLI и Terraform — назначать их на несколько файрволов (Firewall Groups) одновременно. В панели управления можно использовать заранее настроенные шаблоны с правилами для фильтрации трафика, например открыть 22 порт (SSH/TCP), 80 порт (HTTP/TCP), 443 порт (HTTPS/TCP), 1194 порт (OpenVPN/UDP), 3389 порт (RDP/TCP), 20-21 порт (FTP/TCP); открыть стандартные порты для IPsec или WireGuard и другие правила.

Ограничения

На один порт роутера нельзя назначить более одного файрвола.

В одном проекте можно создать не более 10 файрволов. В одном файрволе — две политики, по одной для каждого направления трафика. В одной политике — не более 100 правил.

Если вы настроили NAT (проброс портов), то сначала будет выполняться проброс, а затем действовать правила файрвола.

В Selectel по умолчанию заблокированы некоторые TCP/UDP-порты.

Стоимость

Облачный файрвол предоставляется бесплатно.

Создать облачный файрвол

У облачного файрвола есть базовое свойство: весь входящий и исходящий трафик, который не разрешен, — запрещен. Если создать файрвол без правил и назначить его на порт облачного роутера, весь трафик в подсети роутера будет запрещен. После создания файрвола на роутере прервутся все активные сессии.

1. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.

2. Нажмите **Создать файрвол**.

3. Выберите пул, в котором будет создан файрвол.

4. Опционально: выберите приватную подсеть с облачным роутером, для которой нужно настроить фильтрацию трафика. Файрвол назначается на порт облачного роутера в этой приватной подсети.

   Назначить файрвол на порт роутера можно после создания файрвола.

5. Выберите направление трафика:

   - Входящий трафик
   - Исходящий трафик

6. Если вам подходят шаблоны с правилами для входящего трафика, нажмите на правило. Поля протокола, источника, портов источника, назначения трафика и порта назначения заполнятся автоматически. Перейдите на шаг 14.

7. Если подходящего шаблона нет, добавьте собственное правило для входящего трафика. Нажмите **Добавить правило входящего трафика**.

8. Выберите действие:

   - Allow — разрешить трафик;
   - Deny — отклонить трафик.

9. Выберите протокол: ICMP, TCP, UDP или все протоколы (Any).

10. Введите источник трафика (Source) — IP-адрес, подсеть или все адреса (Any).

11. Введите порт источника (Src. port) — один порт, диапазон портов или все порты (Any).

12. Введите назначение трафика (Destination) — IP-адрес, подсеть или все адреса (Any). Если указать подсеть, то правило будет действовать на все устройства в подсети.

13. Введите порт назначения (Dst. port) — один порт, диапазон портов или все порты (Any).

    Трафик на любой TCP/UDP-порт, заблокированный в Selectel по умолчанию, будет запрещен, даже если указать этот порт в правиле.

14. Введите имя правила или оставьте имя, созданное автоматически.

15. Опционально: введите комментарий для правила.

16. Нажмите **Добавить**. После создания файрвола можно изменить правило.

17. Проверьте порядок правил, они выполняются по порядку в списке — сверху вниз. При необходимости измените порядок — перетащите правила. После создания файрвола можно изменить порядок правил.
18. Опционально: чтобы добавить к файрволу другое правило, перейдите на шаг 5. Можно добавить до 100 правил на каждое направление трафика.
19. Введите имя файрвола или оставьте имя, созданное автоматически.
20. Опционально: введите комментарий для файрвола.
21. Нажмите **Создать файрвол**.

Назначить облачный файрвол на порт облачного роутера и отключить от порта

Назначить файрвол на порт роутера

На один порт роутера нельзя назначить более одного файрвола.
Входящий и исходящий трафик, который не разрешен в правилах облачного файрвола, будет запрещен на порте облачного роутера. На роутере прервутся активные сессии, которые нельзя устанавливать по новым правилам.

1. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.
2. Откройте страницу файрвола → вкладка **Порты**.
3. Нажмите **Назначить на порт**.
4. Выберите приватную подсеть, подключенную к облачному роутеру, для которой нужно настроить фильтрацию трафика.
5. Нажмите **Назначить на порт**.
6. Нажмите **Назначить**.

Отключить файрвол от порта роутера

Правила облачного файрвола перестанут действовать — весь входящий и исходящий трафик, который проходит через порт облачного роутера, будет разрешен.

1. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.
2. Откройте страницу файрвола → вкладка **Порты**.
3. В строке порта роутера нажмите 🗑️.
4. Нажмите **Отключить**.

Управлять правилами облачного файрвола

Для облачного файрвола можно добавить новые правила, изменить существующие правила, изменить порядок правил, а также включать, отключать и удалять правила.

Добавить правило

После добавления запрещающего правила на облачном роутере прервутся активные сессии, которые соответствуют этому правилу.

Можно добавить до 100 правил на каждое направление трафика (политику) для одного облачного файрвола.

5. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.
6. Откройте страницу файрвола.
7. Выберите направление трафика:
8. Входящий трафик
9. Исходящий трафик
10. Откройте вкладку **Входящий трафик**.

11. Нажмите **Создать правило**.

12. Выберите действие:

    a. Allow — разрешить трафик;
    b. Deny — отклонить трафик.
13. Если вам подходят шаблоны с правилами для входящего трафика, выберите правило. Поля протокола, источника, портов источника, назначения трафика и порта назначения заполнятся автоматически. Перейдите на шаг 14.

14. Если подходящего шаблона нет, добавьте собственное правило для входящего трафика.

15. Выберите протокол: ICMP, TCP, UDP или все протоколы (Any).

16. Введите источник трафика (Source) — IP-адрес, подсеть или все адреса (Any).

17. Введите порт источника (Src. port) — один порт, диапазон портов или все порты (Any).

18. Введите назначение трафика (Destination) — IP-адрес, подсеть или все адреса (Any). Если указать подсеть, то правило будет действовать на все устройства в подсети.

19. Введите порт назначения (Dst. port) — один порт, диапазон портов или все порты (Any).

    Трафик на любой TCP/UDP-порт, заблокированный в Selectel по умолчанию, будет запрещен, даже если указать этот порт в правиле.

20. Введите имя правила или оставьте имя, созданное автоматически.

21. Опционально: введите комментарий для правила.

22. Нажмите **Добавить**.

23. Проверьте порядок правил, они выполняются по порядку в списке — сверху вниз. При необходимости измените порядок — перетащите правила. После создания файрвола можно изменить порядок правил.

Изменить правило

После изменения правила на облачном роутере прервутся активные сессии, которые соответствуют измененному правилу.

1. В панели управления перейдите в раздел **Облачная платформа → Файрволы**.

2. Откройте страницу файрвола.

3. Откройте вкладку в зависимости от того, для какого трафика нужно изменить правило:

    - для входящего трафика — **Входящий трафик**;
    - для исходящего трафика — **Исходящий трафик**.
4. В меню ⋮ правила выберите **Изменить правило**.

5. Входящий трафик
6. Исходящий трафик
7. Выберите действие:

    - Allow — разрешить трафик;
    - Deny — отклонить трафик.
8. Если вам подходят шаблоны с правилами для входящего трафика, выберите правило. Поля протокола, источника, портов источника, назначения трафика и порта назначения заполнятся автоматически. Перейдите на шаг 13.

9. Если подходящего шаблона нет, добавьте собственное правило для входящего трафика.

10. Выберите протокол: ICMP, TCP, UDP или все протоколы (Any).

11. Введите источник трафика (Source) — IP-адрес, подсеть или все адреса (Any).

12. Введите порт источника (Src. port) — один порт, диапазон портов или все порты (Any).

13. Введите назначение трафика (Destination) — IP-адрес, подсеть или все адреса (Any). Если указать подсеть, то правило будет действовать на все устройства в подсети.

14. Введите порт назначения (Dst. port) — один порт, диапазон портов или все порты (Any).

    Трафик на любой TCP/UDP-порт, заблокированный в Selectel по умолчанию, будет

запрещен, даже если указать этот порт в правиле.

15. Введите имя правила или оставьте имя, созданное автоматически.
16. Опционально: введите комментарий для правила.
17. Нажмите **Сохранить**.

Изменить порядок правил

После изменения порядка правил на облачном роутере прервутся активные сессии, которые соответствуют новому порядку правил.

1. В панели управления перейдите в раздел **Облачная платформа → Файрволы**.
2. Откройте страницу файрвола.
3. Откройте вкладку в зависимости от того, для какого трафика нужно изменить порядок правил:
    a. для входящего трафика — **Входящий трафик**;
    b. для исходящего трафика — **Исходящий трафик**.
4. Нажмите **Изменить порядок правил**.
5. Перетащите правила. Правила выполняются по порядку в списке — сверху вниз.
6. Нажмите **Сохранить порядок правил**.

Включить правило

1. В панели управления перейдите в раздел **Облачная платформа → Файрволы**.
2. Откройте страницу файрвола.
3. Откройте вкладку в зависимости от того, для какого трафика нужно включить правило:
    - для входящего трафика — **Входящий трафик**;
    - для исходящего трафика — **Исходящий трафик**.
4. В строке с правилом включите правило.

Отключить правило

Правило перестанет действовать — трафик, который был разрешен этим правилом, будет запрещен. На облачном роутере прервутся активные сессии, которые были установлены по этому правилу.

1. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.
2. Откройте страницу файрвола.
3. Откройте вкладку в зависимости от того, для какого трафика нужно отключить правило:
    - для входящего трафика — **Входящий трафик**;
    - для исходящего трафика — **Исходящий трафик**.
4. В строке с правилом отключите правило.

Удалить правило

Правило перестанет действовать — трафик, который был разрешен этим правилом, будет запрещен. На облачном роутере прервутся активные сессии, которые были установлены по этому правилу.

1. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.
2. Откройте страницу файрвола.
3. Откройте вкладку в зависимости от того, для какого трафика нужно удалить правило:
    - для входящего трафика — **Входящий трафик**;
    - для исходящего трафика — **Исходящий трафик**.
4. В меню ⋮ правила выберите **Удалить правило**.
5. Нажмите **Удалить**.

Включить и выключить облачный файрвол

Можно включать или выключать облачный файрвол сразу для всех портов облачного роутера, на которые он назначен.

Чтобы включить или выключить фильтрацию трафика на определенном порте роутера, назначьте файрвол на этот порт или отключите файрвол от порта.

Включить файрвол

Входящий и исходящий трафик, который не разрешен в правилах файрвола, будет запрещен. На облачном роутере прервутся активные сессии, которые нельзя устанавливать по новым правилам.

1. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.

2. Откройте страницу файрвола.
3. В меню ⋮ файрвола выберите **Включить файрвол**.
4. Введите имя файрвола для подтверждения включения.
5. Нажмите **Включить**.

Выключить файрвол

Правила файрвола перестанут действовать — весь входящий и исходящий трафик будет разрешен.

1. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.
2. Откройте страницу файрвола.
3. В меню ⋮ файрвола выберите **Выключить файрвол**.
1. Введите имя файрвола для подтверждения выключения.
2. Нажмите **Выключить**.

Посмотреть статус облачного файрвола

1. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.

2. Посмотрите статус в строке файрвола.

ACTIVE	Файрвол включен, назначен как минимум на один порт роутера и работает
CREATING	Файрвол создается
CREATED	Файрвол создан
INACTIVE	Файрвол не назначен ни на один порт
DOWN	Файрвол выключен
UPDATING	Файрвол обновляется после изменения списка правил
DELETING	Файрвол удаляется
ERROR	Произошла ошибка в работе файрвола. Чтобы исправить ошибку, создайте тикет

Удалить облачный файрвол

При удалении файрвола правила перестанут действовать — весь входящий и исходящий трафик будет разрешен.

Облачный файрвол нельзя удалить, если он находится в статусе `ACTIVE` — включен и назначен на порт облачного роутера.

1. Выключите файрвол или отключите его от порта облачного роутера.
2. В панели управления перейдите в раздел **Облачная платформа** → **Файрволы**.
3. Откройте страницу файрвола.
4. В меню ⋮ файрвола выберите **Удалить файрвол**.
5. Нажмите **Удалить**.

Образы

Образы

Образ — это точная копия файловой системы диска и его содержимого. Из образов можно создавать облачные серверы или создавать загрузочные диски для облачных серверов.

Можно использовать:

- готовые образы — образы с предустановленной операционной системой, которые подготовили специалисты Selectel;
- собственные образы — образы, которые можно самостоятельно загрузить в хранилище образов.

Работать с образами можно в панели управления, с помощью OpenStack CLI или Terraform.

Также для создания серверов можно использовать приложения.

Готовые образы

Готовые образы подготовлены специалистами Selectel. Для каждого готового образа выполнена подготовка рабочего окружения, настройка необходимых параметров и сборка. Образы полностью совместимы с облачной платформой.

Посмотреть актуальный список готовых образов можно в панели управления: в разделе **Облачная платформа** → **Серверы** → нажмите **Создать сервер** → блок **Источник** → нажмите на источник по умолчанию → вкладка **Готовые образы**.

Собственные образы

Если для создания облачного сервера вам нужен образ, которого нет в списке готовых, то вы можете загрузить свой образ в хранилище образов.

С помощью собственных образов можно переносить серверы из других облачных платформ или внутри облачной платформы Selectel, а из образов диска — клонировать облачные серверы.

Поддерживаются форматы образов `.aki`, `.ami`, `.ari`, `.iso`, `.raw`, `.qcow2`, `.vdi`, `.vhd`, `.vhdx` и `.vmdk`. Для некоторых образов формата `.ami` (образы Amazon Machine Image для запуска сервера) требуется дополнительная загрузка образов `.aki` (образ ядра Amazon) и `.ari` (образ оперативной памяти Amazon).

Поддерживаются форматы контейнеров `.aki`, `.ami`, `.ari`, `.bare`, `.ova`, `.ovf`.

Стоимость

Готовые образы входят в стоимость облачных серверов и дополнительно не оплачиваются.

Стоимость хранения собственного образа зависит от его размера и пула, в который он загружен. Хранение собственных образов оплачивается по модели оплаты облачной платформы.

Цены на хранение образов можно посмотреть на selectel.ru.

Загрузить и создать образ

В хранилище образов Selectel можно загрузить образы:

- из файла;
- по ссылке;
- через объектное хранилище;
- формата vmdk.

Можно создать собственный образ из диска.

Ограничения

При загрузке образа в хранилище образов Selectel из файла и по ссылке есть ограничения на размер образа, они зависят от пула. Можно загрузить образ размера:

- до 2048 ГБ (2 ТБ) — в пуле ru-2;
- до 1024 ГБ (1 ТБ) — в других пулах.

Если нужно загрузить образ из файла большего размера, загрузите его через объектное хранилище.

Создать образ можно из диска размера:

- до 2048 ГБ (2 ТБ) — в пуле ru-2;
- до 1024 ГБ (1 ТБ) — в других пулах.

Загрузить образ из файла

В хранилище образов Selectel образ можно загрузить из файла с локального компьютера. Посмотрите ограничения на размер загружаемого образа.

1. В панели управления перейдите в раздел **Облачная платформа** → **Образы**.
2. Нажмите **Создать образ**.

3. Введите имя образа.
4. Выберите сегмент пула, в который загрузится образ.

   Образы размера менее 16 ГБ автоматически реплицируются в соседние сегменты в пуле.
5. Выберите операционную систему.
6. Выберите файл в качестве источника образа.
7. Нажмите **Загрузить**.
8. Выберите формат образа или формат контейнера. Подробнее о форматах в подразделе Собственные образы.

   Если вы загружаете архив с форматом контейнера `.ova`, мы рекомендуем распаковать архив перед загрузкой, чтобы образ работал корректно.

   Если вы не знаете, какие форматы указать, укажите формат образа `raw`, контейнера — `bare`.
9. Опционально: отметьте чекбокс **Указать минимальный объем диска и памяти**. Укажите минимальное количество оперативной памяти в МБ и объем дисков в ГБ. При создании облачного сервера из этого образа панель управления или API автоматически проверят эти ограничения.
10. Нажмите **Создать**.

Загрузить образ по ссылке

В хранилище образов Selectel образ можно загрузить через публичную ссылку на файл с образом. Посмотрите ограничения на размер загружаемого образа.

1. В панели управления перейдите в раздел **Облачная платформа → Образы**.
2. Нажмите **Создать образ**.
3. Введите имя образа.
4. Выберите сегмент пула, в который загрузится образ.

   Образы размера менее 16 ГБ автоматически реплицируются в соседние сегменты в пуле.

5. Выберите операционную систему.
6. Выберите URL в качестве источника образа.
7. Введите ссылку на файл с образом в формате `https://domain.com/file.raw`.
8. Выберите формат образа или формат контейнера. Подробнее о форматах в подразделе Собственные образы.

   Если вы загружаете архив с форматом контейнера `.ova`, мы рекомендуем распаковать архив перед загрузкой, чтобы образ работал корректно.

   Если вы не знаете, какие форматы указать, укажите формат образа `raw`, контейнера — `bare`.
9. Опционально: отметьте чекбокс **Указать минимальный объем диска и памяти**. Укажите минимальное количество оперативной памяти в МБ и объем дисков в ГБ. При создании облачного сервера из этого образа панель управления или API автоматически проверят эти ограничения.
10. Нажмите **Создать**.

Загрузить образ через объектное хранилище

1. Загрузите образ в объектное хранилище через сегментированную загрузку.
2. Получите токен Keystone.
3. В выводе запроса скопируйте значение `X-Subject-Token`.
4. Откройте CLI на локальном компьютере.
5. Создайте запрос на создание образа:

```
Unset

curl 'https://<pool>.cloud.api.selcloud.ru/image/v2/images'
\
  -H 'X-Auth-Token: <keystone_token>' \
  -H 'Content-Type: application/json;charset=utf-8' \
  --data
'{"name":"<image_name>","disk_format":"<image_format>","con
tainer_format":"<container_format>"}'
```

Укажите:

- `<pool>` — пул, в который загрузится образ, например `ru-1`. Адрес (URL) зависит от региона и пула, можно посмотреть в списке URL. Список доступных пулов можно посмотреть в таблице Инфраструктура Selectel;
- `<keystone_token>` — токен Keystone, который вы скопировали на шаге 3;
- `<image_name>` — имя образа;
- `<image_format>` — формат образа. Подробнее о форматах образов в подразделе Собственные образы. Если вы не знаете, какой формат указать, укажите `raw`;
- `<container_format>` — формат контейнера. Подробнее о форматах контейнеров в подразделе Собственные образы.

  Если вы загружаете архив с форматом контейнера `.ova`, мы рекомендуем распаковать архив перед загрузкой, чтобы образ работал корректно.

  Если вы не знаете, какой формат указать, укажите `bare`.

6. В выводе запроса скопируйте значение `id`.
7. Получите ссылку на образ в объектном хранилище.
8. Загрузите образ в хранилище образов:

```
Unset
curl
'https://<pool>.cloud.api.selcloud.ru/image/v2/images/<imag
e_id>/import' \
  -X POST \
  -H 'Content-Type: application/octet-stream' \
  -H 'X-Image-Meta-Store: <pool_segment>' \
  -H 'X-Auth-Token: <keystone_token>' \
  --data-raw
'{"method":{"name":"web-download","uri":"<object_storage_ur
l>"}}'
```

Укажите:

- `<pool>` — пул, в который загрузится образ, например `ru-1`. Адрес (URL) зависит от региона и пула, можно посмотреть в списке URL. Список доступных пулов можно посмотреть в таблице Инфраструктура Selectel;
- `<image_id>` — ID образа, который вы скопировали на шаге 6;
- `<pool_segment>` — сегмент пула, в который загрузится образ, например `ru-1a`. Список доступных сегментов пула можно посмотреть в таблице Инфраструктура Selectel;
- `<keystone_token>` — токен Keystone, который вы скопировали на шаге 3;
- `<object_storage_url>` — ссылка на образ в объектном хранилище вида `https://<uuid>.selstorage.ru/container_name/object_name`, которую вы получили на шаге 7.

Создать образ из диска

Образ — это полная копия диска. Образ можно создать из любого локального или сетевого диска облачного сервера. Диск может быть как загрузочным, так и дополнительным. Посмотрите ограничения на размер диска, из которого можно создать образ.

Можно использовать образ:

- для быстрой настройки одинаковых облачных серверов — клонирования сервера. Если на сервере установлена операционная система и программное обеспечение, то из образа загрузочного диска можно развернуть уже настроенные серверы. Это быстрее, чем настройка нужной конфигурации нескольких серверов;
- изменения типа загрузочного диска;
- переноса сервера в другие пулы, проекты или аккаунты;
- экспорта диска облачного сервера;
- если образ, из которого ранее был создан сервер, оказался удален, можно создать образ из диска сервера и при необходимости создать такой же облачный сервер.

1. Если диск подключен к облачному серверу, мы рекомендуем выключить облачный сервер — из работающего диска может создаться неконсистентный образ.

2. В панели управления перейдите в раздел **Облачная платформа** → **Образы**.

3. Нажмите **Создать образ**.

4. Введите имя образа.

5. Выберите сегмент пула, в который загрузится образ.

   Образы размера менее 16 ГБ автоматически реплицируются в соседние сегменты в пуле.

6. Выберите операционную систему.

7. Выберите диск в качестве источника образа.

8. Выберите диск, из которого будет создан образ. Образ можно создать только в том сегменте пула, в котором находится диск.

9. Опционально: отметьте чекбокс **Указать минимальный объем диска и памяти**. Укажите минимальное количество оперативной памяти в МБ и объем дисков в ГБ. При создании облачного сервера из этого образа панель управления или API автоматически проверят эти ограничения.

10. Нажмите **Создать**.

Перенести (скопировать) образ и настроить общий доступ к образу

Созданный или загруженный образ можно:

- перенести (скопировать) в другой сегмент пула, проект или аккаунт — будет создан новый образ, которым можно управлять в исходном проекте и в проекте-получателе. Хранение всех копий образа оплачивается;
- или настроить доступ к образу между проектами внутри одного пула — управлять образом можно будет только в исходном проекте. Оплачивается хранение образа только в исходном проекте.

11. В обоих случаях из образов можно будет создавать облачные серверы и диски.

Перенести (скопировать) образ в другой сегмент пула, проект или аккаунт
Чтобы скопировать образ, нужно получить его URL и создать из него новый образ. Напрямую перенести образ нельзя.
Образ можно скопировать в другой сегмент пула (в том числе, в другой зоне доступности или регионе), проект или аккаунт. При копировании образа в другой проект или аккаунт можно также изменить сегмент пула. Если вам нужно скопировать образ внутри одного сегмента пула, настройте доступ к образу между проектами — будет оплачиваться хранение только исходного образа.
Хранение всех копий образа оплачивается по модели оплаты облачной платформы.
Управлять образом и создавать из него облачные серверы и диски можно и в исходном проекте, и в проекте-получателе.
После копирования вы можете удалить исходный образ из хранилища образов.

1. В панели управления перейдите в раздел **Облачная платформа → Образы**.

2. В меню ⋮ образа выберите **Скопировать URL образа**.

3. Откройте меню проектов (название текущего проекта) и выберите проект-получатель, в который нужно скопировать образ.

4. Нажмите **Создать образ**.

5. Введите имя образа.

6. Выберите сегмент пула, в который загрузится образ.

   Образы размером менее 16 ГБ автоматически реплицируются в соседние сегменты в пуле.

7. Выберите операционную систему.

8. Выберите URL в качестве источника образа.

9. Введите ссылку, которую вы скопировали на шаге 2.

10. Выберите формат образа или формат контейнера. Подробнее о форматах в подразделе Собственные образы.

    Если вы не знаете, какие форматы указать, укажите формат образа `raw`, контейнера — `bare`.

11. Опционально: отметьте чекбокс **Указать минимальный объем диска и памяти**. Укажите минимальное количество оперативной памяти в МБ и объем дисков в ГБ. При создании облачного сервера из этого образа панель управления или API автоматически проверят эти ограничения.

12. Нажмите **Создать**.

13. Опционально: удалите исходный образ из хранилища образов.

Настроить доступ к образу между проектами

Вы можете настроить общий доступ к образу между проектами внутри одного аккаунта. В проекте-получателе из образа можно будет создавать облачные серверы и диски, а управлять образом можно будет только в исходном проекте: переименовать, изменить операционную систему, удалить образ. Оплачивается хранение образа только в исходном проекте — по модели оплаты облачной платформы.
Можно настроить доступ к образу только внутри пула.
В проекте-получателе можно отключить доступ к образу.

1. В панели управления перейдите в раздел **Облачная платформа**.

2. Скопируйте ID проекта-получателя, в который нужно скопировать образ. Для этого откройте меню проектов (название текущего проекта) и в строке нужного проекта нажмите ⿻.
3. Убедитесь, что вы находитесь в проекте, в котором находится образ. Для этого откройте меню проектов (название текущего проекта) и выберите исходный проект.
4. Перейдите в раздел **Облачная платформа** → **Образы**.
5. Откройте карточку образа.
6. Нажмите **Добавить проект**.
7. Вставьте ID проекта-получателя, который вы скопировали на шаге 2.
8. Нажмите ✓.
9. Скопируйте UUID образа.
10. Откройте меню проектов (название текущего проекта) и выберите проект-получатель.
11. Перейдите в раздел **Облачная платформа** → **Образы**. Убедитесь, что вы выбрали пул, в который нужно перенести образ.
12. На странице раздела нажмите ⇒.
13. Вставьте UUID образа, который вы скопировали на шаге 9.
14. Нажмите **Получить образ**.

Подготовить ISO-образ для работы с облачной платформой

Если вы загрузили в хранилище образов ISO-образ с дистрибутивом операционной системы, мы рекомендуем сделать его полностью совместимым с облачной платформой Selectel. Из совместимого образа можно создавать облачные серверы, для которых будет доступна такая же функциональность, как у серверов из готовых образов.

Это инструкция для образа Oracle Linux. Для других дистрибутивов могут отличаться утилиты, репозитории и расположение файлов.

1. Загрузите ISO-образ в хранилище образов.
2. Создайте облачный сервер из загруженного образа.
3. Настройте облачный сервер.
4. Создайте образ из загрузочного диска облачного сервера.

Скачать образ

Собственный образ можно скачать из хранилища образов только в формате `.raw`.

При необходимости после скачивания вы можете переформатировать образ на локальном компьютере.

1. В панели управления перейдите в раздел **Облачная платформа** → **Образы**.
2. В карточке образа нажмите ⬇.

Удалить образ

Собственный образ можно:

- удалить из хранилища образов — образ полностью удалится и перестанет оплачиваться;
- или отключить к нему доступ в проекте, если к образу был настроен доступ между проектами.

Удалить образ из хранилища

После удаления образ нельзя восстановить. Если к образу настроен доступ между проектами, образ удалится во всех проектах.

1. В панели управления перейдите в раздел **Облачная платформа** → **Образы**.
2. Если к образу настроен доступ между проектами, откройте меню проектов (название текущего проекта) и выберите исходный проект, в который изначально был загружен образ.
3. В меню ⋮ образа выберите **Удалить образ**.
4. Введите имя образа для подтверждения удаления.
5. Нажмите **Удалить**.

Отключить доступ к образу в проекте

Если к образу настроен доступ между проектами, можно отключить доступ к нему в проекте-получателе. После отключения образ будет доступен в исходном проекте и не удалится из хранилища образов. Хранение образа в исходном проекте продолжит оплачиваться по модели оплаты облачной платформы.

1. В панели управления перейдите в раздел **Облачная платформа** → **Образы**.
2. Откройте меню проектов (название текущего проекта) и выберите проект-получатель, для которого был настроен доступ к образу.
3. В меню ⋮ образа выберите **Отказаться**.

Приложения

Для создания облачных серверов можно использовать образы с приложениями и предустановленной операционной системой.

Для каждого образа с приложением выполнена подготовка рабочего окружения, настройка необходимых параметров и сборка.

При использовании облачных серверов с приложениями оплачиваются только ресурсы облачной платформы по модели оплаты облачной платформы.

Перед созданием сервера пополните баланс.

Цены на ресурсы можно посмотреть на selectel.ru.

Доступные приложения и минимальные требования

	Минимальные требования к ресурсам			
	vCPU	**RAM**	**Загрузочный диск**	**Дополнительный диск**
Cloud Gitlab 16.7.4 64-bit, 16.11.3 64-bit	4	8 ГБ	20 ГБ	30 ГБ
Cloud Gitlab Runner 16.5.0 64-bit, 17.0.0 64-bit	2	2 ГБ	8 ГБ	Можно не использовать
Cloud Jitsi Meet stable-9364 64-bit	4	8 ГБ	10 ГБ	Можно не использовать
Cloud Keycloak 24.0.5 64-bit	2	4 ГБ	30 ГБ	Можно не использовать
Cloud Wazuh 4.7.3 64-bit	4	8 ГБ	16 ГБ	Можно не использовать
ISPmanager Lite 6.100.1 Ubuntu 22.04 LTS 64-bit	1	2 ГБ	20 ГБ	Можно не использовать
Nextcloud 27	4	8 ГБ	16 ГБ	50 ГБ
Containers Ready 27.0.3 64-bit	2	2 ГБ	20 ГБ	Можно не использовать

Mattermost	2	4 ГБ	20 ГБ	Можно не использовать
Pritunl	1	1 ГБ	10 ГБ	Можно не использовать
Zabbix	2	8 ГБ	20 ГБ	Можно не использовать

Посмотреть актуальный список приложений можно в панели управления: в разделе **Облачная платформа** → **Серверы** → нажмите **Создать сервер** → блок **Источник** → нажмите на источник по умолчанию → вкладка **Приложения**.

GitLab и GitLab Runner

GitLab — платформа с открытым исходным кодом для хранения репозиториев проектов и автоматизации CI/CD с помощью встроенных пайплайнов и системы отслеживания ошибок. GitLab поддерживает полный цикл CI/CD — непрерывную интеграцию, сборку, тестирование и развертывание кода.

GitLab Runner — открытое программное обеспечение, используется для автоматизации и выполнения задач (пайплайнов) в GitLab CI/CD. Работает как агент, который последовательно выполняет шаги, определенные в задачах пайплайна. Позволяет запускать сборку, тестирование и развертывание приложений в автоматическом режиме, управляя всем процессом выполнения задач CI/CD в GitLab.

Можно создать облачный сервер с готовым приложением GitLab и приложением GitLab Runner.

Jitsi Meet

Jitsi Meet — это полностью зашифрованное решение с открытым исходным кодом для организации видеоконференций.

Можно создать облачный сервер с готовым приложением Jitsi Meet.

Keycloak

Keycloak — платформа с открытым исходным кодом для управления аутентификацией и авторизацией пользователей в приложениях и реализации Single-Sign On.

Можно создать облачный сервер с готовым приложением Keycloak.

Wazuh

Wazuh — это SIEM-система для защиты информации и управления событиями безопасности. Предотвращает и находит уязвимости с помощью агента безопасности, обнаруживает угрозы и реагирует на инциденты.

Можно создать облачный сервер с готовым приложением Wazuh.

ispmanager

ispmanager — панель управления веб-серверами и сайтами. В ispmanager можно управлять доменами, DNS, почтой, базами данных и пользователями, устанавливать CMS и сертификаты, настраивать редиректы, редактировать файлы и выполнять другие задачи.

Можно создать облачный сервер с готовым приложением ispmanager. Мы предоставляем версию ispmanager Lite — можно добавить не более десяти доменов.

Nextcloud и ONLYOFFICE

Nextcloud — платформа с открытым исходным кодом для создания хранилища данных: обмена данными и их синхронизации, работы с документами и файлами. Пользователи Nextcloud могут полностью контролировать свои данные.

ONLYOFFICE — сервис с открытым исходным кодом для совместной работы над документами: редактирования, рецензирования, контроля версий.

Можно создать облачный сервер с готовыми приложениями Nextcloud и ONLYOFFICE.

Containers Ready

Для работы с файлами Docker Compose можно использовать приложение Containers Ready с настроенной операционной системой Ubuntu 22.04. Приложение Containers Ready содержит:

- Docker версии 27.0.3 — платформу контейнеризации для разработки и запуска приложений;
- плагины для запуска Docker Compose версии 2.11.1;
- Portainer версии 2.20.3 — графический интерфейс для мониторинга и управления Docker-контейнерами, образами и сетью Docker.

Для стабильной работы образа в качестве репозитория Docker Registry используется зеркало Selectel.

Можно создать облачный сервер с готовым приложением Containers Ready.

Mattermost

Mattermost — это мессенджер с открытым исходным кодом для обмена мгновенными сообщениями. Можно использовать как альтернативу другим мессенджерам (например, Rocket.Chat) в качестве корпоративного внутреннего чата в компаниях. В Mattermost можно обмениваться файлами и автоматизировать рутинные действия с помощью сценариев.

Mattermost можно развернуть локально или в облаке — создать облачный сервер с готовыми приложением Mattermost.

Pritunl

Pritunl — программное обеспечение с открытым исходным кодом для создания VPN-инфраструктуры. Позволяет создать безопасное и удобное подключение к локальной сети по типу site-to-site.

Можно создать облачный сервер с готовым приложением Pritunl, а затем настроить на нем VPN-сервер. После настройки VPN-сервера пользователи смогут подключиться к VPN.

Zabbix

Zabbix — это открытое программное решение распределенного мониторинга параметров сети, а также состояния и работоспособности серверов.

Можно создать облачный сервер с готовым приложением Zabbix.

Бэкапы

Бэкапы сетевых дисков

Вы можете создавать бэкапы сетевых дисков облачных серверов двумя способами:

- настроить автоматическое создание бэкапов по расписанию. Создайте план бэкапов, укажите расписание создания бэкапов и добавьте в план сетевые диски — подробнее в подразделе Настроить бэкапы по расписанию. Можно настроить создание по расписанию полных или инкрементальных бэкапов;
- вручную — зафиксировать состояние системы и хранить бэкап удаленно от диска. Для создания бэкапа вручную не нужно настраивать план — подробнее в подразделе Создать бэкап вручную. Вручную можно создать только полный бэкап.

Сервис работает на базе компонентов OpenStack Karbor и Cinder.

Посмотреть альтернативные способы создания резервных копий облачных серверов можно в таблице Способы резервного копирования.

Полный бэкап

Полный бэкап — это полная резервная копия диска со всеми данными.

Полные бэкапы можно создавать автоматически по расписанию и вручную.

Можно настроить расписание создания полных бэкапов по дням недели или через cron-выражение. В настройках плана указывается, сколько последних бэкапов хранить.

Инкрементальный бэкап

Инкрементальный бэкап — это копия изменений между текущим состоянием диска и предыдущим бэкапом, созданным по плану. Такой бэкап создается быстрее, чем полный, и занимает меньше места, потому что хранит только изменения на диске.

Инкрементальные бэкапы можно создавать только автоматически по расписанию.

Инкрементальные бэкапы создаются ежедневно во время, которое указывается в настройках плана бэкапа. Первым создается полный бэкап, затем он создается раз в неделю. В остальные дни создаются инкрементальные бэкапы.

Создание бэкапов

Мы гарантируем консистентность копий на уровне crash-consistency. В момент создания в бэкап записываются данные, которые есть на диске. Также в бэкап могут записываться «грязные данные», которые появляются при перезаписи или удалении файлов на диске. Данные в памяти облачного сервера не записываются в бэкап. Из-за «грязных данных» размер полного бэкапа может превышать реальный объем данных и файлов на диске;

инкрементального — превышать разницу между текущим объемом данных и размером предыдущего бэкапа.

Создание бэкапа не влияет на производительность облачного сервера — все операции происходят на вычислительных мощностях Selectel. При создании полного бэкапа создается мгновенный снимок диска, роста нагрузки на облачном сервере не происходит. При создании инкрементального бэкапа изменения между текущим состоянием диска и предыдущим бэкапом вычисляются на лету, а разница между состояниями переносится в хранилище бэкапов.

Хранение бэкапов

Полные и инкрементальные бэкапы хранятся в хранилище Ceph — в каждом сегменте пула развернут кластер. В одном кластере хранятся и бэкапы, и диски — так увеличивается скорость создания бэкапа и восстановления из него.

Бэкапы хранятся на отдельных серверах в трех копиях — это позволит сохранить данные, если случится проблема с серверами, на которых находятся диски.

Бэкап нельзя скачать, но из него можно восстановить диск — будет создан новый диск такого же типа и размера, как исходный.

Бэкапы, которые автоматически создаются по расписанию, хранятся цепочками по семь штук — один полный и шесть последующих инкрементальных. В плане указывается, сколько полных бэкапов хранить (минимум — два). Например, если в настройках плана указано хранение трех полных бэкапов, то будут храниться три последние цепочки бэкапов.

Ограничения хранения бэкапов

Если бэкапы создаются автоматически по расписанию, общее количество бэкапов в одном проекте не ограничено. При этом в рамках одного плана есть ограничение на создание: для планов с полными бэкапами — 90 бэкапов, для планов с инкрементальными — 14 полных бэкапов и 78 инкрементальных.

В одном проекте можно хранить не более 1000 бэкапов, созданных вручную.

Автоматическое удаление бэкапов

Только для бэкапов, которые созданы автоматически по расписанию.

В настройках плана указывается, какое количество последних полных бэкапов или цепочек инкрементальных бэкапов хранить. Когда для диска создается новый полный бэкап, сервис проверяет суммарное количество полных бэкапов диска в рамках одного плана. Если это количество больше, чем максимальное количество, указанное в плане, то удаляются наиболее старые полные бэкапы.

Инкрементальные бэкапы хранятся цепочками по семь бэкапов — один полный и шесть последующих инкрементальных. Через неделю после создания первого полного бэкапа

самый ранний инкрементальный бэкап объединяется с самым ранним полным бэкапом. Если в настройках плана вы указали хранение двух полных бэкапов, будет храниться две последние цепочки, если три полных бэкапа — три последние цепочки и так далее.

Все бэкапы сохранятся, если вы удалите диск, облачный сервер или план бэкапов.

Бэкапы можно удалить вручную.

Стоимость

Хранение бэкапов оплачивается по модели оплаты облачной платформы.

Стоимость хранения бэкапов зависит от размера бэкапа и сегмента пула, в котором он хранится. Оплачивается хранение бэкапов только со статусами `AVAILABLE` или `RESTORING`, бэкапы в других статусах не оплачиваются.

Оплачивается каждый ГБ хранения бэкапов. Если размер бэкапа меньше 1 ГБ, оплачиваемый объем округляется до 1 ГБ.

Например, вы храните бэкап размером 512 МБ в сегменте пула ru-9a. Стоимость хранения бэкапа будет равна стоимости хранения 1 ГБ в этом сегменте пула — 3,66 ₽ в месяц.

Стоимость одного ГБ хранения бэкапов можно посмотреть на selectel.ru.

Посмотреть фактический размер бэкапа можно в панели управления в разделе **Облачная платформа** → **Бэкапы** → вкладка **Бэкапы**. Посмотреть суммарный объем бэкапов, которые оплачиваются, можно в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Текущая стоимость**.

Создать бэкапы

Можно создать бэкап вручную или настроить автоматическое создание бэкапов по расписанию.
Подробнее о полных и инкрементальных бэкапах в инструкции Бэкапы сетевых дисков.
У бэкапов нет автоматической проверки работоспособности и консистентности копий. Мы рекомендуем периодически восстанавливаться из бэкапов — так вы сможете проверить, что восстановление работает корректно.

Создать бэкап вручную

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. В меню ⋮ диска выберите **Создать бэкап**.
3. Нажмите **Создать бэкап**.

Настроить бэкапы по расписанию

Настройки резервного копирования диска можно задать в плане бэкапов:

- к каким дискам применить план — для каких дисков будут создаваться бэкапы по этому плану;
- тип создаваемых бэкапов — полные или инкрементальные;
- расписание — когда будут создаваться бэкапы диска;
- сколько последних полных бэкапов нужно хранить — подробнее о хранении бэкапов.
- Один план бэкапов можно применить к одному диску или нескольким сразу — вы можете не настраивать расписание бэкапов для каждого диска отдельно. К одному диску можно применить любое количество планов.
  У диска можно изменить список планов, которые к нему применяются.
  Если необходимо изменить настройки резервного копирования, можно отредактировать план.

Создать план

1. В панели управления перейдите в раздел **Облачная платформа** → **Бэкапы**.
2. Откройте вкладку **Планы**.
3. Нажмите **Создать план**.
4. Введите имя плана.
5. Выберите сегмент пула, в котором находится диск.
6. Отметьте диски, к которым применится план.
7. Выберите тип бэкапа: полный или инкрементальный.
8. Если вы выбрали полный бэкап, укажите, как настраивать расписание.
   - По дням недели
   - Через cron-выражение
9. Чтобы настроить создание бэкапов по дням недели, отметьте нужные дни и введите время в формате `ЧЧ:ММ` в вашем часовом поясе, в которое будут создаваться бэкапы.
10. Если вы выбрали инкрементальный бэкап, ведите время в формате `ЧЧ:ММ` в вашем часовом поясе, в которое ежедневно будут создаваться бэкапы.

    Первым создается полный бэкап, затем он создается ровно через неделю и далее

раз в неделю. В остальные дни создаются инкрементальные бэкапы.

11. Укажите, какое количество последних полных бэкапов нужно хранить:
    - для полных бэкапов минимальное количество — один;
    - для инкрементальных бэкапов минимальное количество хранящихся полных бэкапов — два. Инкрементальные бэкапы хранятся цепочками по семь бэкапов — один полный и шесть последующих инкрементальных. Например, если в настройках плана указано хранение трех полных бэкапов, то будут храниться три последние цепочки бэкапов.
12. Максимальное количество бэкапов, которое можно создать в рамках одного плана, ограничено: для полных — 90 бэкапов, для инкрементальных — 14 полных бэкапов и 78 инкрементальных.

13. Нажмите **Создать план**.

Изменить список планов

К диску можно добавить любое количество планов, по которому будут создаваться бэкапы, и отключить от него планы.

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. В меню ⋮ диска выберите **Настроить план бэкапов**.
3. Чтобы добавить новый план, выберите существующий план или нажмите **Новый план** и создайте новый.
4. Чтобы отключить план, в строке плана нажмите **Отключить**.

Редактировать план

Тип бэкапов в плане изменить нельзя.

1. В панели управления перейдите в раздел **Облачная платформа** → **Бэкапы**.
2. Откройте вкладку **Планы**.
3. В меню ⋮ плана выберите **Изменить настройки**.
4. Опционально: измените диски, к которым применяется план. При отключении плана от диска созданные для него бэкапы сохранятся.
5. Опционально: измените расписание создания бэкапов.
6. Опционально: измените количество хранящихся бэкапов. Если вы уменьшите это количество, то после автоматического создания новых бэкапов предыдущие бэкапы, которые не попадают под новое ограничение, удалятся. Например, вместо хранения семи бэкапов вы установили хранение четырех — после создания одного нового бэкапа первые четыре бэкапа будут удалены (останется один новый и три предыдущих).
7. Нажмите **Сохранить**.

Восстановиться из бэкапа

При восстановлении из бэкапов сетевых дисков создается новый диск с таким же типом и объемом, как исходный.

Время восстановления бэкапа зависит от объема бэкапа. Например, бэкап объемом 100 ГБ восстановится за 11 минут. Во время восстановления сетевой диск, для которого был создан бэкап, будет находиться в статусе `RESTORING-BACKUP`.

Восстановиться из бэкапа на исходный диск или на новый облачный сервер невозможно. Восстановленный диск можно подключить к облачному серверу или создать из него новый сервер.

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. В меню ⋮ диска выберите **Восстановить диск из бэкапа**.
3. Выберите точку восстановления — это момент времени, в который был создан бэкап.
4. Введите имя нового диска.
5. Нажмите **Создать диск**.

Посмотреть статус бэкапа

1. В панели управления перейдите в раздел **Облачная платформа** → **Бэкапы**.
2. Откройте вкладку **Бэкапы**.
3. Посмотрите статус в строке бэкапа.

PROTECTING	Бэкап создается
AVAILABLE	Бэкап успешно создан, из него можно восстановить данные. Бэкапы в этом статусе оплачиваются
RESTORING	Данные бэкапа восстанавливаются на диск. Бэкапы в этом статусе оплачиваются
ERROR	При создании бэкапа произошла ошибка
ERROR-DELETING	При удалении бэкапа произошла ошибка
DELETING	Бэкап удаляется

Отключить автоматическое создание бэкапов

Отключить автоматическое создание бэкапов по расписанию можно несколькими способами:

- остановить план — план и его настройки сохранятся, создание бэкапов по нему остановится. План можно будет включить позже;
- отключить план от диска — по этому плану перестанут создаваться бэкапы определенного диска. Диск к плану можно будет подключить позже;
- удалить план — по такому плану перестанут создаваться бэкапы, план нельзя будет восстановить.

Остановить план

Если вам нужно временно приостановить создание бэкапов по плану и при этом сохранить его настройки, остановите выполнение плана.

Ранее созданные бэкапы сохранятся. План можно будет включить позже.

1. В панели управления перейдите в раздел **Облачная платформа** → **Бэкапы**.
2. Откройте вкладку **Планы**.
3. В меню ⁝ плана выберите **Остановить выполнение**.
4. Опционально: чтобы заново включить план, в меню ⁝ плана выберите **Включить план**.

Отключить план от диска

Можно отключить план от определенного диска — по нему перестанут создаваться бэкапы.

Ранее созданные бэкапы сохранятся. План можно будет включить позже.

Если план включен для нескольких дисков и вы отключите план от одного, план продолжит работать для оставшихся дисков.

1. В панели управления перейдите в раздел **Облачная платформа** → **Диски**.
2. В меню ⁝ диска выберите **Настроить бэкапы**.
3. В строке с планом нажмите **Отключить**.

Удалить план

После удаления плана по нему перестанут создаваться бэкапы.

Ранее созданные бэкапы сохранятся.

1. В панели управления перейдите в раздел **Облачная платформа** → **Бэкапы**.
2. Откройте вкладку **Планы**.
3. В меню ⁝ плана выберите **Удалить план**.

Удалить бэкап

Полные бэкапы можно удалять по одному.
Инкрементальные бэкапы удаляются только цепочкой бэкапов, созданных в рамках одного плана. При удалении одного любого бэкапа из цепочки — инкрементального или

полного — удалятся все бэкапы в цепочке.
Бэкап можно удалить, если он находится в статусе `AVAILABLE` или `ERROR`. Для цепочки бэкапов все бэкапы должны иметь эти статусы. Если нужно удалить бэкапы в других статусах, создайте тикет.

1. В панели управления перейдите в раздел **Облачная платформа** → **Бэкапы**.
2. В меню ⋮ бэкапа выберите **Удалить бэкап**.
3. Введите название бэкапа для подтверждения удаления.
4. Нажмите **Удалить**.

Резервное копирование облачных серверов

Selectel предоставляет услуги уровня инфраструктуры, поэтому для облачных серверов резервное копирование по умолчанию не выполняется.

Вы можете настроить автоматическое резервное копирование или сделать копию вручную. Посмотреть инструменты можно в таблице Способы резервного копирования.

Альтернативный способ создания копий — использовать скрипты и утилиты на облачном сервере, подробнее в подразделе Решения для хранения копий.

Балансировщики нагрузки

Общая информация

Облачный балансировщик нагрузки распределяет входящий сетевой трафик между облачными серверами в одном пуле. Балансировщик нагрузки можно использовать для повышения доступности сервисов — он оптимально распределит запросы между серверами и снизит нагрузку. Если один сервер выйдет из строя, балансировщик перенаправит трафик на другой подходящий сервер.

Балансировщик работает на уровнях L3-L4 (network load balancer) и L7 (application load balancer). Для балансировки HTTPS-трафика используются TLS(SSL)-сертификаты из менеджера секретов, подробнее в инструкции TLS(SSL)-сертификаты балансировщика нагрузки.

Работать с балансировщиком нагрузки можно в панели управления, через OpenStack CLI или Terraform.

Для отслеживания метрик балансировщика вы можете настроить мониторинг с использованием Prometheus, подробнее о доступных метриках и настройке мониторинга в инструкции Мониторинг облачного балансировщика нагрузки.

Типы балансировщика нагрузки

	Базовый без резервирования	**Базовый с резервированием**	**Продвинутый с резервированием**
Количество инстансов	Один	Два	Два
Конфигурация инстанса	2 vCPU, 1 ГБ RAM	2 vCPU, 1 ГБ RAM	4 vCPU, 2 ГБ RAM
Отказоустойчивость и резервирование	Только Single-режим	Аварийное переключение (Active-Standby Failover) на резервный инстанс в одном пуле	Аварийное переключение (Active-Standby Failover) на резервный инстанс в одном пуле

Для чего подойдет	Для тестовых окружений или проектов, для которых не нужна доступность сервиса 24 / 7	Для небольших и средних проектов, для которых критична доступность сервиса	Для проектов с высокой нагрузкой и требованием к постоянной доступности сервиса
Пропускная способность	До 3 Гбит/с. Можно увеличить до 5 Гбит/с — создайте тикет	До 3 Гбит/с. Можно увеличить до 5 Гбит/с — создайте тикет	До 3 Гбит/с. Можно увеличить до 5 Гбит/с — создайте тикет
Количество HTTP-запросов в секунду (RPS)	~19 500	~19 500	~34 000
Количество HTTPS-запросов с терминацией на балансировщике в секунду (RPS)	~3 000 keep-alive подключений (при 10 000 одновременных подключений по TCP)	~3 000 keep-alive подключений (при 10 000 одновременных подключений по TCP)	~9 000 keep-alive подключений (при 10 000 одновременных подключений по TCP)

Если типы не подходят, вы можете заказать кастомный тип балансировщика — создайте тикет.

Как работает балансировщик нагрузки

В балансировщике нагрузки используется модель OpenStack Octavia, которая включает в себя:

- инстанс (amphora) — выполняет балансировку нагрузки. Запускается на облачном сервере и использует HAProxy (High-Availability Proxy) — программное обеспечение для проксирования трафика. В балансировщиках с резервированием (типов Базовый с резервированием и Продвинутый с резервированием) создается два инстанса, без резервирования — один;
- целевая группа (pool) — группа серверов, к которой правило перенаправляет запросы по указанному для группы протоколу;
- серверы (members) — серверы, которые обслуживают трафик в пуле. Доступны по IP-адресу и порту, которые указаны для сервера в рамках целевой группы;
- проверки доступности (health monitor) — процесс проверки работоспособности всех серверов в целевой группе;

- правило (listener) — прослушивает поступающий на балансировщик нагрузки поток трафика, используя указанные в правиле протоколы и порты. Затем маршрутизирует трафик к необходимой группе серверов;
- HTTP-политика (L7 Policy) — дополнительные условия в правиле для маршрутизации HTTP-трафика с определенными параметрами.

Целевые группы

Целевая группа — группа серверов, на которые распределяется трафик с балансировщика нагрузки. Сервер может входить в несколько целевых групп одного балансировщика, если в этих группах для сервера указаны разные порты.

Для целевой группы можно настроить:

- протоколы и порты для приема трафика от балансировщика нагрузки;
- алгоритмы, по которым распределяются запросы;
- проверки доступности для отслеживания состояния серверов.

Проверки доступности

Для целевой группы можно включить проверку доступности. Балансировщик будет отслеживать состояние серверов — если какой-либо сервер окажется неработоспособным, балансировщик перенаправит соединение на другой.

Параметры проверки:

- тип проверки. В зависимости от протокола целевой группы доступны типы:
    - группа TCP — TCP, PING;
    - группа PROXY — TLS-HELLO, HTTP, TCP, PING;
    - группа UDP — UDP-CONNECT, PING;
    - группа HTTP — HTTP, TCP, PING;
- для протокола проверки HTTP можно настроить обращение к URL и ожидаемые коды ответа;
- интервал между проверками — интервал в секундах, с которым балансировщик отправляет проверяющие запросы серверам;
- таймаут соединения — время ожидания ответа;
- порог успеха — количество успешных обращений подряд, после которых сервер переводится в рабочее состояние;
- порог неуспеха — количество неуспешных обращений подряд, после которых работа сервера приостанавливается.

Правила

Правило — настройки балансировщика, которые обслуживают поток трафика с конкретным портом и протоколом и распределяют этот трафик на нужную группу серверов.

В правиле можно настроить:

- протоколы и порты входящего трафика балансировщика нагрузки;
- HTTP-политики для дополнительной маршрутизации HTTP-трафика;
- соединения, проходящие через балансировщик;
- выбрать целевую группу серверов.

Количество правил в балансировщике не ограничено.

HTTP-политики

HTTP-политика — дополнение в правиле, которое позволяет маршрутизировать определенный HTTP- и HTTPS-трафик отдельно от остального трафика:

- направлять на другую целевую группу (REDIRECT_TO_POOL);
- направлять на URL — полностью заменять URL запроса, включая протокол, доменное имя, путь и параметры запроса (REDIRECT_TO_URL);
- направлять на префикс URL — заменять протокол и доменное имя в URL запроса (REDIRECT_PREFIX);
- отклонять (REJECT).

Запрос перенаправляется по первой подходящей политике. Порядок применения политик зависит от действия политики: сначала применяются политики REJECT, затем REDIRECT_TO_URL и REDIRECT_PREFIX, затем REDIRECT_TO_POOL. Если в правиле несколько политик с одинаковым действием, они применяются согласно позиции политики в правиле. Вы можете изменить порядок применения политик.

HTTP-политика состоит из набора условий, количество условий в политике не ограничено. Чтобы запрос попал под политику, он должен соответствовать всем условиям политики. В условии указываются:

- параметр запроса для проверки: `HOST_NAME` или `PATH`. При настройке политики через Openstack CLI также можно создать условие по параметрам `COOKIE`, `FILE_TYPE` и `HEADER`;
- контрольное значение для проверки — точное значение или регулярное выражение;
- тип совпадения с контрольным значением: `EQUAL TO`, `STARTS WITH`, `ENDS WITH`, `CONTAINS`, `REGEX`.

Количество HTTP-политик в правиле не ограничено.

Порты балансировщика нагрузки

Инстансы балансировщика нагрузки используют несколько портов:

- входящий порт (uplink). Это виртуальный порт, на котором размещается VIP — виртуальный IP-адрес. На нем правило прослушивает входящий трафик. Выделяется при создании балансировщика нагрузки и находится в его подсети. У балансировщиков с резервированием (типов Базовый с резервированием и Продвинутый с резервированием) VIP резервируется по протоколу VRRP;
- служебные VRRP-порты. При создании базового балансировщика нагрузки в его подсети выделяется один служебный порт. При создании балансировщика с резервированием выделяется два служебных порта для основного и резервного инстанса, между ними настраивается VRRP;
- служебные порты (downlinks). Если серверы находятся не в подсети балансировщика, то при его создании в подсетях с серверами выделяются порты для инстансов: для базового балансировщика один порт, для балансировщиков с резервированием — два порта (основной и резервный).

При неполадках в работе балансировщика нагрузки он автоматически создает новый инстанс и только потом удаляет старый — для этого нужен свободный порт. Если свободного порта не будет, балансировщик перейдет в статус `ERROR`.

Если при создании балансировщика нагрузки вы выбрали в качестве подсети балансировщика публичную подсеть и будете размещать в ней серверы, то убедитесь, что в ней есть дополнительный IP-адрес, или используйте публичную сеть размером от /28.

Мы рекомендуем выбирать приватную сеть с публичным IP-адресом (адрес нужен для доступа в интернет) — в таком случае для пересоздания инстанса всегда будет доступен свободный IP-адрес. Балансировка трафика будет производиться внутри приватной сети.

Протоколы

Доступны комбинации протоколов:

- TCP–TCP — классическая L4-балансировка;
- TCP–PROXY — информация о клиенте не теряется и передается в отдельном заголовке соединения;
- UDP–UDP — UDP-протокол быстрее, чем TCP, но менее надежен;
- HTTP–HTTP — L7-балансировка;
- HTTPS–HTTP — L7-балансировка с шифрованием и терминацией SSL-сертификата на балансировщике.

Алгоритмы распределения запросов

Правило распределяет запросы по выбранному алгоритму. Доступно два алгоритма:

- Round Robin — алгоритм кругового обслуживания. Первый запрос передается одному серверу, следующий запрос — другому и так далее до достижения последнего сервера. Затем цикл начинается сначала. Запросы распределяются на серверы в соответствии с заданным весом.

- Least connections — алгоритм учитывает количество подключений к серверам. Новый запрос передается серверу с наименьшим количеством активных подключений, вес сервера не учитывается.

Sticky Sessions

Дополнительно можно включить Sticky Sessions. Метод необходим, когда конечное приложение держит длительное соединение с каждым клиентом и сохраняет внутреннее состояние данных, которое не синхронизируется между серверами в правиле.

Новые запросы будут распределяться по выбранному алгоритму, а затем сессия закрепится за сервером, который начал обрабатывать запросы. Все последующие запросы этой сессии будут распределяться на сервер, не учитывая выбранный алгоритм. Если сервер недоступен, запрос перенаправится на другой.

Параметры определения сессии можно настроить — балансировать сессии или балансировать одного клиента на один сервер. Можно идентифицировать сессию:

- по APP-cookie — уже существующая cookie, которая задана в коде приложения;
- по HTTP-cookie — cookie, которую создает и прикрепляет к сессии балансировщик;
- по Source IP — IP-адрес клиента хешируется и делится на вес каждого сервера в целевой группе — так определяется сервер, который будет обрабатывать запросы.

Настройки соединений

Можно задать настройки соединений, проходящих через балансировщик, — между входящими запросами и балансировщиком, балансировщиком и серверами.

Настройки соединений:

- таймаут соединения — время ожидания ответа;
- максимум соединений — максимальное количество активных соединений;
- таймаут неактивности — время, в течение которого подключение считается активным, даже если данные не передаются;
- таймаут ожидания TCP-пакетов — время, в течение которого балансировщик ждет передачи данных для инспекции по уже установленному соединению.

Заголовки HTTP-запросов

В обычном режиме работы балансировщик передает серверу только исходное тело HTTP-запроса, заменяя IP-адрес клиента на свой.

Включите необходимые типы дополнительных заголовков в запрос, чтобы серверы получали эту информацию для корректной работы или анализа:

- `X-Forwarded-For` — IP-адрес, с которого пришел запрос;
- `X-Forwarded-Port` — порт балансировщика, на который пришел запрос;
- `X-Forwarded-Proto` — исходный протокол соединения;

- `X-SSL-Client-Verify` — использовал ли клиент защищенное соединение;
- `X-SSL-Client-Has-Cert` — наличие сертификата у клиента;
- `X-SSL-Client-DN` — идентификационная информация владельца;
- `X-SSL-Client-CN` — имя хоста, для которого выпущен сертификат;
- `X-SSL-Issuer` — центр сертификации, в котором был выпущен сертификат;
- `X-SSL-Client-SHA1` — SHA1-отпечаток клиентского сертификата;
- `X-SSL-Client-Not-Before` — начало действия сертификата;
- `X-SSL-Client-Not-After` — окончание действия сертификата.

Стоимость

Балансировщики оплачиваются по модели оплаты облачной платформы.

Стоимость балансировщиков можно посмотреть на selectel.ru.

Создать балансировщик нагрузки

1. Выберите конфигурацию и сеть.
2. Создайте целевую группу.
3. Создайте правила и HTTP-политики.

1. Выбрать конфигурацию и сеть

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Балансировщики**.
3. Нажмите **Создать балансировщик**.
4. Выберите регион и пул, в котором будет создан балансировщик.
5. Выберите конфигурацию в зависимости от нагрузки на проект.
6. Введите имя балансировщика.
7. Опционально: введите комментарий — любую дополнительную информацию о балансировщике, она будет отображаться только в панели управления.
8. Выберите подсеть:
    - приватную — балансировка трафика будет производиться только внутри подсети. Можно подключить публичный IP-адрес к приватному адресу — балансировщик будет доступен из интернета через NAT;
    - или публичную — балансировщик будет доступен из интернета и сможет проксировать запросы из публичной подсети к облачным серверам в

приватной подсети. Если вы будете размещать облачные серверы в этой же подсети, то выберите сеть размером от /28 или убедитесь, что в ней есть свободный IP-адрес для порта балансировщика нагрузки.

9. Укажите IP-адрес в подсети — свободный адрес, который будет назначен на балансировщик.

10. Опционально: подключите публичный IP-адрес. Если нет свободного публичного IP-адреса, создайте новый IP-адрес. Приватная подсеть, в которой вы создаете балансировщик, должна быть подготовлена для подключения публичного IP-адреса.

11. Нажмите **Дальше**.

2. Создать целевую группу

1. Откройте вкладку **Серверы**.

2. Опционально: чтобы изменить имя целевой группы, нажмите □, введите имя и нажмите ✓.

3. Выберите протокол назначения трафика, по которому балансировщик будет передавать трафик на целевую группу. Доступны следующие комбинации протоколов для приема трафика на балансировщике и назначения трафика на целевую группу:

    - TCP–TCP — классическая L4-балансировка;
    - TCP–PROXY — информация о клиенте не теряется и передается в отдельном заголовке соединения;
    - UDP–UDP — UDP-протокол быстрее, чем TCP, но менее надежен;
    - HTTP–HTTP — L7-балансировка;
    - HTTPS–HTTP — L7-балансировка с шифрованием и терминацией SSL-сертификата на балансировщике.

4. Для выбранного протокола будет автоматически выбран стандартный порт — измените его при необходимости. Значение порта будет общим для всех серверов в группе.

5. Отметьте серверы, которые добавятся в целевую группу.

6. Укажите настройки для каждого отмеченного сервера:

    6.1. Выберите IP-адрес.

    6.2. Опционально: измените порт.

    6.3. Укажите вес сервера — это пропорциональная мера, обозначает долю запросов, которую обрабатывает сервер. Если значения весов одинаковые, то серверы обслуживают равное количество запросов. Если, например, в группе один

сервер с весом «2» и два сервера с весом «1», то первый сервер получит 50% всех запросов, а другие два — по 25%. Максимальное значение веса — 256.

6.4. Опционально: чтобы направлять трафик на сервер только при недоступности остальных серверов в группе, отметьте чекбокс **Резервный**.

7. Откройте вкладку **Алгоритм**.

8. Выберите алгоритм распределения запросов — Round Robin или Least connections.

9. Опционально: чтобы включить метод Sticky Sessions, отметьте чекбокс **Sticky sessions** и выберите идентификатор сессии. Для идентификатора APP-cookie введите имя cookie.

10. Откройте вкладку **Проверки доступности**.

11. Выберите тип проверки доступности. После создания группы тип проверки изменить нельзя.

12. Если выбран тип проверки HTTP, укажите параметры запроса — метод, путь и ожидаемые коды ответа.

13. Укажите интервал между проверками — интервал в секундах, с которым балансировщик отправляет проверяющие запросы серверам.

14. Укажите таймаут соединения — максимальное время ожидания ответа в секундах, должно быть меньше интервала между проверками.

15. Укажите порог успеха — количество успешных обращений подряд, после которых сервер переводится в рабочее состояние.

16. Укажите порог неуспеха — количество неуспешных обращений подряд, после которых работа сервера приостанавливается.

17. Опционально: чтобы добавить еще одну целевую группу, нажмите **Добавить целевую группу** и настройте ее.

18. Нажмите **Дальше**.

3. Создать правила и HTTP-политики

1. Выберите протокол приема трафика на балансировщике — TCP, UDP, HTTP или HTTPS. Доступен также вариант Prometheus для настройки мониторинга балансировщика нагрузки.
    - TCP- или UDP-трафик
    - HTTP- или HTTPS-трафик

2. Для выбранного протокола будет автоматически выбран стандартный порт, на котором балансировщик будет слушать трафик, — измените его при необходимости.

3. Выберите целевую группу. Доступны группы, на которые можно балансировать трафик по выбранному протоколу приема трафика.

4. Опционально: разверните блок **Расширенные настройки правила** и укажите настройки соединений:

    - для входящих запросов на балансировщик — укажите таймаут соединения и максимум соединений;
    - для запросов от балансировщика к серверам — укажите таймаут соединения, таймаут неактивности и таймаут ожидания TCP-пакетов.
5. Опционально: чтобы добавить еще одно правило, нажмите **Добавить правило** и перейдите на шаг 1. Количество правил не ограничено.

6. Проверьте итоговую стоимость балансировщика.

7. Нажмите **Создать балансировщик**.

Работа с балансировщиком нагрузки

Выключить балансировщик

Если балансировщик выключен, он продолжает оплачиваться.

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики** → вкладка **Балансировщики**.
2. В меню ⁝ балансировщика выберите **Выключить балансировщик**. Балансировщик перейдет в статус `OFFLINE`.

Включить балансировщик

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики** → вкладка **Балансировщики**.
2. В меню ⁝ балансировщика выберите **Включить балансировщик**. Балансировщик перейдет в статус `ACTIVE`.

Подключить публичный IP-адрес к балансировщику нагрузки

Статический публичный IP-адрес можно подключить при создании балансировщика или в уже созданном балансировщике.

1. Создайте публичный IP-адрес в пуле, в котором находится балансировщик нагрузки.
2. Если балансировщик нагрузки находится в приватной подсети, подключите подсеть к облачному роутеру. Проверьте, что роутер подключен к внешней сети.
3. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики** → вкладка **Балансировщики**.
4. В карточке балансировщика нажмите **Подключить публичный IP-адрес**. Выберите публичный IP-адрес.

TLS(SSL)-сертификаты балансировщика нагрузки

Для работы с HTTPS-трафиком на балансировщик необходимо добавить TLS(SSL)-сертификат, чтобы балансировщик мог читать HTTPS-запросы и использовать информацию протокола HTTP для правильной балансировки. Терминация TLS-сертификата происходит на балансировщике, балансировщик передает данные серверам по HTTP.
Балансировщик нагрузки работает с TLS(SSL)-сертификатами из менеджера секретов. Вы можете:

- выпустить бесплатный Let's Encrypt® сертификат, в том числе Wildcard (для домена и поддоменов);
- добавить пользовательский сертификат, поддерживаются сертификаты с опциями SAN (один сертификат для нескольких доменов) и Wildcard.

Сертификаты с пустым полем `CN` (Common Name) не поддерживаются в балансировщиках нагрузки.
При перевыпуске или обновлении сертификата в менеджере он автоматически обновится на балансировщике. Сессии со старым сертификатом будут прерваны и переустановлены с новым сертификатом в течение трех часов после обновления сертификата. Для большинства протоколов переустановка сессий происходит незаметно для конечных пользователей.
Сертификат добавляется при создании правила. В панели управления для правила можно выбрать только один сертификат. Если вам нужно добавить в правило несколько сертификатов, сертификаты нужно добавить через Openstack CLI.

Добавить несколько TLS(SSL)-сертификатов для балансировщика

1. Добавьте TLS(SSL)-сертификаты в менеджере секретов — выпустите Let's Encrypt® сертификаты или загрузите пользовательские. Сертификаты с пустым полем `CN` (Common Name) не поддерживаются в облачных балансировщиках нагрузки.
   Откройте OpenStack CLI.

2. Добавьте сертификаты — создайте новое правило для балансировщика нагрузки или обновите существующее:

```
Unset
openstack loadbalancer listener create \
  -v --protocol-port 443 \
  --protocol TERMINATED_HTTPS \
  --name <listener_name> \
  --default-tls-container=<certificate_uuid_1> \
  --sni-container-refs <certificate_uuid_1>
<certificate_uuid_2> \
  -- <loadbalancer>
```

   Укажите:

   - `<listener_name>` — имя правила;
   - `<certificate_uuid_1>`, `<certificate_uuid_2>` — ID сертификатов. Можно скопировать в панели управления: в разделе **Облачная платформа** → **Менеджер секретов** → вкладка **Сертификаты** → в меню ⋮ сертификата выберите **Скопировать UUID**;
   - `<loadbalancer>` — ID или имя балансировщика. Список можно посмотреть с помощью `openstack loadbalancer list`

Посмотреть статус балансировщика нагрузки

Для балансировщика отображается два статуса:

- статус работы — показывает статус балансировки трафика;
- статус конфигурации инстанса — показывает статус применения последних настроек в балансировщике.

Посмотреть статус работы балансировщика нагрузки

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Балансировщики**.
3. Посмотрите статус в карточке балансировщика нагрузки.

ONLINE	Баласировщик работает, все целевые группы принимают трафик по заданным правилам
OFFLINE	Балансировщик не обрабатывает запросы и выключен
DEGRADED	В целевых группах балансировщика есть недоступные серверы, но все группы продолжают принимать трафик
ERROR	Одна из целевых групп перестала принимать запросы, либо произошла ошибка в работе балансировщика. Если все серверы работают корректно и находятся в статусе `ONLINE`, создайте тикет
NO_MONITOR	В целевых группах балансирощика не включены проверки доступности. Если все серверы балансировщика в этом статусе, то статус балансировщика ≠ `ONLINE`

Посмотреть статус конфигурации инстанса

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Балансировщики**.
3. Посмотрите статус в карточке балансировщика нагрузки в поле **Статус конфигурации инстанса**.

ACTIVE	Последние настройки успешно применились на балансировщике
CREATING	Создается баланировщик или объект в нем (правило, HTTP-политика, целевая группа или сервер в ней)
UPDATING	На балансировщике применяются ваши последние настройки
ERROR	При применении настроек произошла ошибка, балансировка трафика идет по старым настройкам. Попробуйте изменить настройки повторно, если ошибка сохраняется — создайте тикет
DELETING	Балансировщик удаляется

Мониторинг облачного балансировщика нагрузки

Для облачных балансировщиков нагрузки можно настроить мониторинг — собирать и экспортировать метрики OpenStack Octavia в формате Prometheus и подключить Grafana, чтобы отслеживать метрики на дашбордах.

Посмотреть список доступных метрик можно в таблице Метрики Octavia в формате Prometheus.

Настроить мониторинг

Мы не рекомендуем настраивать мониторинг в период максимальной нагрузки вашей инфраструктуры. При увеличении трафика на балансировщике нагрузки растет частота запроса метрик — это влияет на производительность инстансов балансировщика.

1. Создайте правило балансировщика нагрузки.
2. Создайте облачный сервер для Prometheus и Grafana.
3. Установите Prometheus на облачном сервере и настройте сбор метрик.
4. Установите Grafana на облачном сервере и авторизуйтесь в Grafana.
5. Создайте дашборд в Grafana.

Посмотреть статистику балансировщика нагрузки

1. В панели управления перейдите в раздел **Облачная платформа → Балансировщики**
2. Откройте вкладку **Балансировщики**.
3. В меню ⋮ балансировщика выберите **Статистика**.
4. Посмотрите доступную статистику по балансировщику.

Активные соединения	Текущее количество активных соединений между входящими запросами и балансировщиком и между балансировщиком и серверами
Всего соединений	Общее количество соединений, установленных через балансировщик с момента его создания, без учета соединений по удаленным правилам
Принято	Объем трафика, принятого балансировщиком
Отправлено	Объем трафика, переданного балансировщиком

Ошибки HTTP-запросов	Количество ошибок на стороне клиента при обращении к серверам за балансировщиком. Учитываются, например, следующие ошибки: • клиент прервал сессию до отправки запроса к серверу; • произошла ошибка при чтении данных от клиента; • таймаут на стороне клиента; • клиент разорвал соединение; • получено несколько некорректных запросов от клиента; • к запросу была применена политика Tarpit

Удалить балансировщик нагрузки

Вместе с балансировщиком будут удалены его правила и целевые группы. Облачные серверы, которые входят в группы, не удалятся.

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**
2. Откройте вкладку **Балансировщики**.
3. В меню ⋮ балансировщика нагрузки выберите **Удалить балансировщик**.
4. Для подтверждения удаления введите имя балансировщика нагрузки.
5. Нажмите **Удалить**.

Работа с целевыми группами

Создать целевую группу

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Целевые группы**
3. Нажмите **Создать целевую группу**.
4. Выберите регион и пул, где будет создана целевая группа. Балансировщик и целевая группа должны находиться в одном пуле.
5. Выберите балансировщик нагрузки.
6. Выберите протокол назначения трафика, по которому балансировщик будет передавать трафик на целевую группу. Доступны следующие комбинации

протоколов для приема трафика на балансировщике и передачи трафика на целевую группу:

   - TCP–TCP — классическая L4-балансировка;
   - TCP–PROXY — информация о клиенте не теряется и передается в отдельном заголовке соединения;
   - UDP–UDP — UDP-протокол быстрее, чем TCP, но менее надежен;
   - HTTP–HTTP — L7-балансировка;
   - HTTPS–HTTP — L7-балансировка с шифрованием и терминацией SSL-сертификата на балансировщике.

7. Для выбранного протокола будет автоматически выбран стандартный порт — измените его при необходимости. Значение порта будет общим для всех серверов в группе.

8. Откройте вкладку **Серверы**.

9. Отметьте серверы, которые добавятся в целевую группу.

10. Укажите настройки для каждого отмеченного сервера:

    10.1. Выберите IP-адрес.

    10.2. Опционально: измените порт.

    10.3. Укажите вес сервера — это пропорциональная мера, обозначает долю запросов, которую обрабатывает сервер. Если значения весов одинаковые, то серверы обслуживают равное количество запросов. Если, например, в группе один сервер с весом «2» и два сервера с весом «1», то первый сервер получит 50% всех запросов, а другие два — по 25%. Максимальное значение веса — 256.

    10.4. Опционально: чтобы направлять трафик на сервер только при недоступности остальных серверов в группе, отметьте чекбокс **Резервный**.

11. Откройте вкладку **Алгоритм**.

12. Выберите алгоритм распределения запросов — Round Robin или Least connections.

13. Опционально: чтобы включить метод Sticky Sessions, отметьте чекбокс **Sticky sessions**.

14. Откройте вкладку **Проверки доступности**.

15. Выберите тип проверки доступности. После создания группы тип проверки изменить нельзя.

16. Если выбран тип проверки HTTP, укажите параметры запроса — метод, путь и ожидаемые коды ответа.

17. Укажите интервал между проверками — интервал в секундах, с которым балансировщик отправляет проверяющие запросы серверам.

18. Укажите таймаут соединения — время ожидания ответа в секундах, должно быть меньше интервала между проверками.

19. Укажите порог успеха — количество успешных обращений подряд, после которых сервер переводится в рабочее состояние.

20. Укажите порог неуспеха — количество неуспешных обращений подряд, после которых работа сервера приостанавливается.

21. Опционально: измените имя целевой группы или оставьте сформированное по умолчанию.

22. Опционально: введите комментарий к группе.

23. Нажмите **Создать целевую группу**.

Добавить сервер в целевую группу

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Целевые группы** → страница целевой группы.
3. В блоке **Серверы** нажмите **Добавить сервер**.
4. Выберите сервер.
5. Выберите IP-адрес.
6. Для сервера будет автоматически выбрано значение порта группы — измените его при необходимости.
7. Укажите вес сервера — это пропорциональная мера, обозначает долю запросов, которую обрабатывает сервер. Если значения весов одинаковые, то серверы обслуживают равное количество запросов. Если, например, в группе один сервер с весом «2» и два сервера с весом «1», то первый сервер получит 50% всех запросов, а другие два — по 25%. Максимальное значение веса — 256.
8. Если нужно сделать сервер резервным, чтобы он принимал запросы только при недоступности остальных серверов группы, отметьте чекбокс **Резервный**.
9. Нажмите ✓.

Сделать сервер в группе резервным

Облачный сервер в целевой группе можно сделать резервным — он будет включен в группу, но перестанет принимать запросы, пока будет доступен хотя бы один сервер в группе. Если все серверы в группе будут недоступны, резервный сервер включится в работу.

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.

2. Откройте вкладку **Целевые группы** → страница целевой группы.
3. В блоке **Серверы** в строке сервера включите тумблер в столбце **Резервный**.

Приостановить сервер в группе

Приостановить сервер можно при проведении работ на сервере, например, при обновлении приложения или перезагрузке — сервер временно не будет обрабатывать запросы для этой целевой группы. Сам сервер при этом продолжит работать.

Удалять сервер из целевой группы не нужно — он продолжит обработку трафика, как только вы возобновите его работу.

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Целевые группы** → страница целевой группы.
3. В блоке **Серверы** в меню ⁝ сервера выберите **Не принимать запросы**.

Возобновить работу сервера в группе

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Целевые группы** → страница целевой группы.
3. В блоке **Серверы** в меню ⁝ сервера выберите **Принимать запросы**.

Удалить сервер из целевой группы

Если вы удалите сервер из целевой группы, он перестанет принимать апросы. Сам сервер при этом не удалится.

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Целевые группы** → страница целевой группы.
3. В блоке **Серверы** в меню ⁝ сервера выберите **Удалить сервер из группы**.

Изменить алгоритм распределения запросов

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.

2. Откройте вкладку **Целевые группы** → страница целевой группы.

3. В строке **Алгоритм** нажмите □.

4. Выберите алгоритм:

    - Round Robin — алгоритм кругового обслуживания. Первый запрос передается одному серверу, следующий запрос — другому и так далее до

достижения последнего сервера. Затем цикл начинается сначала. Запросы распределяются на серверы в соответствии с заданным весом.
    - Least connections — алгоритм учитывает количество подключений к серверам. Новый запрос передается серверу с наименьшим количеством активных подключений, вес сервера не учитывается.
5. Опционально: чтобы включить метод Sticky Sessions, в строке **Sticky Sessions** нажмите □, отметьте чекбокс **Sticky Sessions** и выберите идентификатор сессии. Для идентификатора сессии APP-cookie введите имя cookie.

Управлять проверками доступности

У целевой группы может быть только одна проверка доступности.

В проверке доступности можно изменить все параметры, кроме типа проверки. Если нужно изменить тип проверки, вы можете удалить существующую проверку доступности и создать новую с нужным типом через Openstack CLI.

Создать проверку доступности

1. Откройте OpenStack CLI.
2. Создайте проверку доступности:

```
Unset
openstack loadbalancer healthmonitor create \
  --name <name> \
  --delay <delay> \
  --timeout <timeout> \
  --max-retries <max_retries> \
  --max-retries-down <max_retries_down> \
  --type <type> \
  --http-method <http_method> \
  --url-path <url_path> \
  --expected-codes <codes> \
  <pool>
```

Укажите:

- `<delay>` — интервал между проверками в секундах;
- `<timeout>` — время ожидания ответа в секундах;
- `<max_retries>` — количество успешных обращений подряд, после которых сервер переводится в рабочее состояние;
- `<max_retries_down>` — количество неуспешных обращений подряд, после которых работа сервера приостанавливается;
- `<type>` — тип проверки зависимости от протокола целевой группы:
  - группа TCP — `TCP`, `PING`;
  - группа PROXY — `TLS_HELLO`, `HTTP`, `TCP`, `PING`;
  - группа UDP — `UDP_CONNECT`, `PING`;
  - группа HTTP — `HTTP`, `TCP`, `PING`;
- параметры HTTP-запроса, если вы выбрали тип проверки `HTTP`:
  - `--http-method <http_method>` — метод проверки: `GET`, `POST`, `DELETE`, `PUT`, `HEAD`, `OPTIONS`, `PATCH`, `CONNECT`, `TRACE`;
  - `--url-path <url_path>` — путь запроса без доменного имени;
  - `--expected-codes <codes>` — ожидаемые коды ответа через запятую;
- `<pool>` — ID или имя целевой группы, можно посмотреть с помощью `openstack loadbalancer pool list`

Изменить проверку доступности

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Целевые группы** → страница целевой группы.
3. Убедитесь, что тумблер **Проверки доступности** включен.
4. Если тип проверки — HTTP, то вы можете изменить обращение к URL и ожидаемые коды ответа, для этого нажмите **Изменить** и введите новые настройки.
5. Опционально: разверните блок **Расширенные настройки правила** и укажите настройки соединений:
   - для входящих запросов на балансировщик — укажите таймаут соединения и максимум соединений;

- для запросов от балансировщика к серверам — укажите таймаут соединения, таймаут неактивности и таймаут ожидания TCP-пакетов.

6. Нажмите **Сохранить**.

Удалить проверку доступности

Если вы удалите проверку доступности, балансировщик будет направлять трафик на все серверы целевой группы, включая недоступные.

1. Откройте OpenStack CLI.
2. Удалите проверку:

```
Unset
openstack loadbalancer healthmonitor delete <health_monitor>
```

> Укажите `<health_monitor>` — ID или имя проверки доступности, можно посмотреть с помощью `openstack loadbalancer healthmonitor list`

Посмотреть статус целевой группы и серверов

Посмотреть статус целевой группы

Статус работы показывает, как происходит балансировка трафика.

1. В панели управления перейдите в раздел **Облачная платформа → Балансировщики**.
2. Откройте вкладку **Целевые группы**.
3. Посмотрите статус в карточке целевой группы.

ONLINE	Все проверки доступности проходят успешно, серверы принимают запросы
DEGRADED	Часть серверов группы не принимает запросы от балансировщика
ERROR	Все серверы в группе не проходят проверку доступности и не принимают трафик от балансировщика, при этом сами серверы могут быть в активном состоянии

OFFLINE	Все серверы в группе приостановлены и не принимают запросы от балансировщика

Посмотреть статус серверов

1. В панели управления перейдите в раздел **Облачная платформа** → **Целевые группы**.
2. Откройте вкладку **Целевые группы** → страница целевой группы.
3. Посмотрите статус в строке сервера → столбец **Статус**.

ONLINE	Сервер успешно отвечает на проверки доступности
CREATING	Сервер добавляется в целевую группу
UPDATING	Обновляются настройки сервера
OFFLINE	Сервер не принимает запросы, при этом сам сервер может быть в активном состоянии
BACKUP	Сервер переведен в статус резервного и будет включен в работу, если будут неработоспособными остальные серверы в целевой группе
NO_MONITOR	Работоспособность сервиса не проверяется проверками доступности. Если все серверы балансировщика в этом статусе, то статус балансировщика ≠ `ONLINE`
DRAINING	Сервер не принимает новые подключения, но продолжает обрабатывать текущие
ERROR	Сервис на указанном порту не отвечает или не проходит проверку по типу ответа
DELETING	Сервер удаляется из целевой группы балансировщика. Это не влияет на работоспособность сервера

Удалить целевую группу

Если целевая группа используется в HTTP-политике, политика будет удалена вместе с целевой группой. Серверы целевой группы не будут удалены.

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Целевые группы**.

3. В карточке группы нажмите 🗑️.
4. Введите имя целевой группы.
5. Нажмите **Удалить**.

Инструменты для автоматизации

OpenStack CLI

OpenStack CLI — это консольный клиент для работы с OpenStack API. Через OpenStack CLI в Selectel можно управлять облачной инфраструктурой: серверами, группами размещения, сетевыми дисками, сетями, образами и балансировщиками нагрузки.

Документацию по работе с продуктами через OpenStack CLI можно посмотреть на вкладке `OpenStack` в инструкциях, например, Создать облачный сервер или Подключить диск.

Актуальные версии компонентов, которые поддерживаются в Selectel, можно посмотреть в таблице Версии компонентов OpenStack.

OpenStack CLI можно установить в локальной системе.

1. Установите OpenStack CLI и дополнительные пакеты. Если для работы с OpenStack CLI вы хотите использовать Docker-контейнер, этот шаг выполнять не нужно.
2. Создайте сервисного пользователя для авторизации в OpenStack API.
3. Настройте авторизацию в OpenStack API.

Версии компонентов OpenStack

	Версия релиза	Версия API
Keystone	Zed	3.14
Placement	Zed	1.0 (максимальная микроверсия — 1.39)
Nova	Zed	2.1 (максимальная микроверсия — 2.93)
Neutron	Ussuri	2.0
Cinder	Wallaby	3.0 (максимальная микроверсия — 3.64)
Glance	Zed	2.16
Karbor	Wallaby	1.0
Manila	Zed	2.0 (максимальная микроверсия — 2.75)
Heat	Zed	1.0
Octavia	2023.1	2.26
Gnocchi	4.5	1.0

selvpcclient

Библиотеку go-selvpcclient и консольный клиент python-selvpcclient можно использовать для работы с Cloud Management API и Quota Management API: проектами, квотами и другими объектами.

Установить go-selvpcclient

Пакет go-selvpcclient содержит Go-библиотеку.
Посмотреть примеры использования библиотеки можно в документации selvpcclient на pkg.go.dev.

1. Загрузите пакет:

```
Unset
go get github.com/selectel/go-selvpcclient/selvpcclient/v3
```

2. Создайте сервисного пользователя для аутентификации.

Установить python-selvpcclient

Пакет python-selvpcclient содержит консольный клиент selvpc CLI.
Посмотреть примеры использования selvpc CLI можно в документации selvpcclient на GitHub.

1. Получите токен Selectel (ключ API).

2. Установите переменные окружения:

```
Unset
      export SEL_TOKEN=<selectel_token>
      export SEL_URL=https://api.selectel.ru/vpc/resell
      export SEL_API_VERSION=2
      export
      OS_AUTH_URL=https://cloud.api.selcloud.ru/identity/v3
```

Укажите:

- `<selectel_token>` — токен Selectel (ключ API), который вы получили на шаге 1;
- `OS_AUTH_URL` — адрес (URL) зависит от региона и пула, можно посмотреть в списке URL.

3. Загрузите пакет:

```
Unset
pip install -U python-selvpcclient
```

Сети облачной платформы

Общая информация

Сети облачной платформы работают на базе OpenStack Neutron. Подробнее в разделе Neutron документации OpenStack.

Работать с сетями облачной платформы можно в панели управления, с помощью OpenStack CLI или Terraform.

Решаемые задачи

В облачной платформе с помощью сетевых объектов можно:

- настраивать связность между устройствами в одном пуле и объединять в приватные подсети с помощью портов устройства: облачные серверы, балансировщики нагрузки, файловые хранилища, кластеры Managed Kubernetes и кластеры облачных баз данных;
- маршрутизировать трафик между приватными подсетями и настраивать доступ в интернет для устройств в приватной подсети с помощью облачных роутеров;
- подключать статические публичные IP-адреса к устройствам в приватных подсетях, чтобы настроить доступ к ним из интернета;
- подключать устройства к публичным подсетям для доступа в интернет и из интернета. К публичным подсетям можно подключить с помощью портов облачные серверы, балансировщики нагрузки и кластеры облачных баз данных;
- для организации сетевой связности между устройствами в разных пулах (в том числе, в разных проектах и аккаунтах) или между разными услугами приватные подсети можно подключать к глобальному роутеру;
- настраивать статические маршруты для подсетей.

Дополнительно можно распределять трафик входящий сетевой трафик между облачными серверами с помощью балансировщиков нагрузки. Для приватных подсетей и публичных IP-адресов можно настроить фильтрацию трафика с помощью облачных файрволов.

Пропускная способность

В сетевых объектах облачной платформы есть ограничения на объем исходящего и входящего трафика.

Список регионов, зон доступности и пулов можно посмотреть в таблице Инфраструктура Selectel.

Пропускную способность для устройств в приватных сетях можно повысить до 10 Гбит/с — создайте тикет.

Скорость на порте может сильно снизиться, например, до 0,1 Гбит/с, если ассоциированный IP-адрес заблокирован системой безопасности Selectel. Чтобы увеличить скорость, создайте тикет.

Заблокированные порты

В Selectel по умолчанию заблокированы некоторые TCP/UDP-порты, трафик через них заблокирован.

Стоимость

Публичные IP-адреса и публичные подсети оплачиваются по модели оплаты облачной платформы.

Стоимость можно посмотреть на selectel.ru.

Остальные сетевые ресурсы предоставляются бесплатно.

Приватные подсети и сети

Приватные сети — это L2-сегменты сети. В каждой приватной сети должна быть создана хотя бы одна приватная подсеть. Приватные подсети — это диапазоны приватных IP-адресов на уровне L3, ограниченные размером CIDR. Если устройства находятся в разных приватных подсетях одной приватной сети, они могут общаться напрямую.

Внутри разных приватных сетей могут быть подсети с одинаковыми префиксами (масками), но внутри одной сети префиксы подсетей должны быть разными. По умолчанию приватные сети и подсети не имеют доступа в интернет и из интернета, в них нельзя использовать публичную адресацию.

Чтобы приватные подсети из разных сетей могли общаться, их нужно подключить к одному облачному роутеру. Для организации сетевой связности на уровне L3 между устройствами в разных пулах (в том числе, в разных проектах и аккаунтах) или между разными услугами нужно подключить приватные подсети к глобальному роутеру. Адреса подсетей, подключенных к одному роутеру (облачному или глобальному), не должны пересекаться.

По умолчанию приватные сети и принадлежащие им подсети можно использовать только внутри одного проекта и одного пула. Можно настроить общий доступ к приватной сети в разных проектах внутри одного аккаунта.

Внутри приватных подсетей есть ограничения на объем трафика — пропускная способность. Ее можно посмотреть в таблице Пропускная способность.

Работать с приватными подсетями и сетями можно в панели управления, с помощью OpenStack CLI или Terraform.

Автоматические настройки приватной подсети

В приватных подсетях указываются настройки по умолчанию: шлюз по умолчанию и DNS-серверы. Если вы добавляете устройство в существующую подсеть, настройки применяются к нему автоматически. Если вы изменили настройки подсети, в которой уже

есть устройства, для применения настроек нужно обновить сетевые настройки на всех устройствах в подсети.

Шлюз по умолчанию

При создании приватной подсети для шлюза по умолчанию резервируется первый свободный IP-адрес. Например, для подсети с CIDR `192.168.0.0/24` под шлюз будет зарезервирован `192.168.0.1`. Шлюз по умолчанию можно изменить при создании подсети или изменить после создания.

DNS-серверы

При создании приватной подсети на устройствах в подсети автоматически прописываются DNS-серверы Selectel. DNS-серверы можно изменить при создании подсети или изменить после создания.

Статические маршруты

По умолчанию в подсетях не указаны статические маршруты. Для приватных подсетей можно настроить статические маршруты.

Создать приватную сеть

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Приватные сети**.
3. Нажмите **Создать сеть**.
4. Выберите пул, в котором будет создана приватная сеть.
5. Введите имя сети.
6. Опционально: введите комментарий для сети.
7. Введите CIDR подсети — диапазон IP-адресов, доступных в подсети.
8. Опционально: чтобы изменить IP-адрес шлюза по умолчанию, нажмите . Введите значение. Нажмите ✓.
9. Опционально: чтобы изменить DNS-серверы, нажмите . Введите от одного до трех значений. Нажмите ✓.
10. Опционально: чтобы включить DHCP, отметьте чекбокс **Включить DHCP**.
11. Опционально: чтобы добавить еще одну подсеть, нажмите **Добавить подсеть** и перейдите на шаг 7.
12. Нажмите **Создать**.

Добавить подсеть в приватную сеть

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Приватные сети**.
3. Откройте страницу сети → вкладка **Подсети**.
4. Нажмите **Создать подсеть**.
5. Введите CIDR подсети — диапазон IP-адресов, доступных в подсети.
6. Опционально: измените IP-адрес шлюза по умолчанию.
7. Опционально: измените DNS-серверы. Введите от одного до трех значений.
8. Опционально: чтобы включить DHCP, отметьте чекбокс **Включить DHCP**.

9. Нажмите ✓.

Статические маршруты

Статическую маршрутизацию можно использовать, если в облачной подсети есть устройство, выполняющее роль маршрутизатора. Можно:

- настроить статические маршруты в подсети, в которой находятся устройства, например, облачные серверы;
- настроить статические маршруты на облачном роутере.

Для настройки статических маршрутов на глобальном роутере используйте инструкцию Настроить маршрутизацию на глобальном роутере.

Примеры решаемых задач

Доступ в интернет для сети, подключенной к глобальному роутеру

Например, приватная сеть облачной платформы подключена к глобальному роутеру, и при этом нужно:

- настроить доступ в интернет для облачных серверов, которые находятся в подсетях это приватной сети;
- настроить доступ в интернет для приватной подсети кластера Managed Kubernetes, чтобы развернуть ноды;
- использовать публичный IP-адрес для облачного сервера или для балансировщика нагрузки в приватной сети;
- использовать облачный роутер в качестве шлюза для доступа в интернет для серверов или хостов из других пулов и услуг.

Отправка трафика через облачный сервер (прокси)

Если нужно отправлять трафик до других подсетей, можно использовать облачный сервер как шлюз и настроить статическую маршрутизацию. Например:

- настроить доступ в интернет из подсети;
- настроить связность с внешней инфраструктурой через VPN.

Настроить статические маршруты в подсети

В качестве исходной подсети можно использовать:

- приватную подсеть;
- подсеть глобального роутера;
- публичную подсеть — только через OpenStack CLI;
- приватные сети и публичные подсети, к которым настроен доступ в разных проектах (с тегом `Кросспроектная`) — только через OpenStack CLI.

Для статического маршрута нельзя задать метрику (вес или стоимость маршрута), поэтому невозможно настроить два и более маршрута с одинаковыми исходной подсетью и подсетью назначения.

При настройке статического маршрута в панели управления в качестве исходной подсети можно выбрать приватную подсеть или подсеть глобального роутера.

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Приватные сети**.
3. Откройте карточку приватной сети → вкладка **Статические маршруты**.
4. Нажмите **Добавить маршрут**.
5. Выберите исходную подсеть.
6. Введите CIDR подсети назначения — это подсеть, в которую будет направляться трафик.
7. Введите шлюз (next-hop) — IP-адрес, через который устройства исходной подсети будут направлять трафик в подсеть назначения. Можно ввести любой адрес из исходной подсети.
8. Нажмите **Добавить**.
9. Примените изменения. Для этого обновите сетевые настройки на устройствах в подсети.

Обновить сетевые настройки

Если вы изменили сетевые настройки (DNS-серверы, шлюз по умолчанию, статические маршруты) приватной подсети, в которой есть устройства, для применения настроек нужно обновить сетевые настройки на всех устройствах в подсети.

Обновить сетевые настройки на облачном сервере

Если сначала вы изменили сетевые настройки приватной подсети (DNS-серверы, шлюз по умолчанию, статические маршруты), а затем создали в ней облачные серверы, все настройки на серверах пропишутся автоматически.

Если сначала вы создали облачные серверы, а затем изменили сетевые настройки подсети, для применения настроек:

1. Проверьте DHCP в приватной подсети.
2. Примените новые сетевые настройки на облачном сервере.
3. Измените файлы конфигурации сети облачного сервера.

Обновить сетевые настройки на кластере Managed Kubernetes

Если сначала вы изменили сетевые настройки приватной подсети (DNS-серверы, шлюз по умолчанию, статические маршруты), а затем создали в ней ноды кластера Managed Kubernetes, все настройки на нодах кластера пропишутся автоматически.

Если сначала вы создали ноды кластера Managed Kubernetes, а затем изменили сетевые настройки подсети, для применения настроек последовательно выключите все ноды кластера и включите их.

Обновить сетевые настройки на эластичном файловом хранилище

Если сначала вы изменили сетевые настройки приватной подсети (DNS-серверы, шлюз по умолчанию, статические маршруты), а затем создали в ней эластичное файловое хранилище, все настройки на хранилище пропишутся автоматически.

Если сначала вы создали эластичное файловое хранилище, а затем изменили сетевые настройки подсети, примените изменения.

1. В панели управления перейдите в раздел **Облачная платформа → Файловое хранилище**.
2. Откройте страницу эластичного файлового хранилища → вкладка **Настройки**.
3. Нажмите **Обновить настройки сети**.

Порты

Порт — это виртуальная сетевая карта, на которую из подсети назначается связка MAC-адреса и приватного IP-адреса. IP-адрес назначается на порт в рамках подсети, в которой находится порт.

Порты используются для подключения устройств к приватным подсетям, подсетям глобального роутера и публичным подсетям. Если от устройства отключить порт, оно будет отключено и от подсети. Приватную подсеть нельзя удалить, если в ней есть хотя бы один порт.

Работать с портами можно в панели управления, с помощью OpenStack CLI или Terraform.

В облачных сетях автоматически создаются служебные порты, управление ими недоступно:

- два DHCP-порта в приватной подсети. Создаются при включении DHCP в подсети, удаляются при отключении DHCP;
- три служебных порта в подсети глобального роутера для сетевого оборудования. Создаются при подключении приватной сети к глобальному роутеру, удаляются при отключении приватной сети от глобального роутера или при удалении глобального роутера;
- VRRP-порты и downlinks (порты для резервирования) в приватных подсетях, в которых находится балансировщик нагрузки. Количество служебных портов зависит от типа балансировщика, подробнее о портах балансировщика нагрузки;
- порт в приватной подсети, в которой находится эластичное файловое хранилище. Создается вместе с подсетью для эластичного файлового хранилища, можно удалить только с хранилищем.

Добавить порт в подсеть

Порт можно добавить в приватную подсеть, подсеть глобального роутера или публичную подсеть.

2. В панели управления перейдите в раздел **Облачная платформа → Сеть**.
3. Откройте вкладку в зависимости от того, в какую подсеть нужно добавить порт:
   - для приватной подсети или подсети глобального роутера — **Приватные сети**;
   - для публичной подсети — **Публичные сети**.
4. Откройте карточку подсети → вкладка **Порты**.
5. Нажмите **Добавить порт**.

6. Выберите подсеть.
7. Введите IP-адрес порта.
8. Нажмите **Добавить порт**.

Добавить облачный сервер или ноду кластера Managed Kubernetes в подсеть через порт

Облачный сервер после создания сервера можно добавить в приватную подсеть, подсеть глобального роутера или публичную подсеть. Ноду кластера Managed Kubernetes можно добавить в приватную подсеть или подсеть глобального роутера.

Для этого нужно добавить к серверу или ноде порт.

1. В панели управления перейдите в раздел **Облачная платформа → Серверы**.
2. Откройте страницу сервера → вкладка **Порты**.
3. Нажмите **Добавить порт**.
4. Выберите приватную подсеть, подсеть глобального роутера или публичную подсеть.
5. Введите IP-адрес порта.
6. Нажмите **Добавить порт**.

Подключить публичный IP-адрес к порту в приватной подсети

Если к порту в приватной подсети подключен облачный сервер или балансировщик нагрузки, к порту можно подключить публичный IP-адрес.

Для подключения публичного IP-адреса в разделах устройств в панели управления используйте инструкцию Публичные IP-адреса.

1. Убедитесь, что устройство находится в подсети, которая соответствует требованиям. Для подготовки подсети используйте инструкцию Подготовить приватную подсеть для подключения публичного IP-адреса.
2. В панели управления перейдите в раздел **Облачная платформа → Сеть**.
3. Откройте вкладку **Приватные сети**.
4. Откройте страницу сети → вкладка **Порты**.
5. В строке порта облачного сервера или балансировщика нагрузки в столбце **Публичный IP** нажмите **Подключить**.
6. Выберите публичный IP-адрес.

Отключить публичный IP-адрес от порта в приватной подсети

Для отключения публичного IP-адреса в разделах устройств в панели управления используйте инструкцию Публичные IP-адреса.

1. Убедитесь, что устройство находится в подсети, которая соответствует требованиям. Для подготовки подсети используйте инструкцию Подготовить приватную подсеть для подключения публичного IP-адреса.
2. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
3. Откройте вкладку **Приватные сети**.
4. Откройте страницу сети → вкладка **Порты**.
5. В строке порта облачного сервера или балансировщика нагрузки в столбце **Публичный IP** в меню ⋮ публичного IP-адреса выберите **Отключить публичный IP**.
6. Выберите публичный IP-адрес.

Включить порт

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку в зависимости от того, для какой подсети нужно включить порт:
    - для приватной подсети или подсети глобального роутера — **Приватные сети**;
    - для публичной подсети — **Публичные сети**.
3. Откройте карточку подсети → вкладка **Порты**.
4. В строке порта включите порт.

Отключить порт

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку в зависимости от того, для какой подсети нужно отключить порт:
    - для приватной подсети или подсети глобального роутера — **Приватные сети**;
    - для публичной подсети — **Публичные сети**.
3. Откройте карточку подсети → вкладка **Порты**.
4. В строке порта отключите порт.

Удалить порт

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.

2. Откройте вкладку в зависимости от того, порт из какой подсети нужно удалить:

    - для приватной подсети или подсети глобального роутера — **Приватные сети**;
    - для публичной подсети — **Публичные сети**.

3. Откройте карточку подсети → вкладка **Порты**.

4. В строке порта нажмите 🗑️.

5. Если это порт приватной подсети и кнопка 🗑️ неактивна, к порту подключено устройство, запрещающее удаление. Удалите это устройство и вернитесь на шаг 1.

    Для удаления устройства используйте инструкции:

    - удалить облачный роутер;
    - удалить кластер Managed Kubernetes;
    - удалить эластичное файловое хранилище;
    - удалить балансировщик нагрузки.

Облачные роутеры

С помощью облачного роутера можно:

- маршрутизировать трафик между приватными подсетями. Все приватные подсети, подключенные к одному роутеру, могут общаться между собой и использовать IP-адрес роутера как маршрут по умолчанию;
- настроить доступ в интернет для устройств в приватной подсети (исходящий трафик) и из интернета (входящий трафик), подробнее в инструкции Настроить доступ в интернет и из интернета. Облачный роутер выполняет функцию 1:1 NAT через внешний IP-адрес, который выделяется при подключении роутера к внешней сети: организовывает доступ в интернет из приватной подсети и обрабатывает пакеты входящего трафика для публичных IP-адресов.

На облачном роутере можно настроить статические маршруты.
Облачный роутер можно использовать только внутри одного проекта и одного пула.
Для облачных роутеров есть ограничения на объем трафика — пропускная способность. Ее можно посмотреть в таблице Пропускная способность.
Работать с облачными роутерами можно в панели управления, с помощью OpenStack CLI или Terraform.

Создать облачный роутер

2. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
3. Откройте вкладку **Облачные роутеры**.
4. Нажмите **Создать роутер**.
5. Выберите пул, в котором будет создан облачный роутер.
6. Введите имя роутера.
7. Опционально: отметьте чекбокс **Подключить роутер к внешней сети** — для роутера будет выделен внешний IP-адрес.
8. Нажмите **Создать**.

Подключить подсеть к облачному роутеру

Чтобы приватные подсети могли общаться между собой, их нужно подключить к одному облачному роутеру. Подсети должны иметь разные CIDR.
Чтобы настроить доступ в интернет и из интернета для устройств в приватных подсетях с помощью облачного роутера, используйте инструкцию Настроить доступ в интернет и из интернета.

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. Откройте карточку роутера.

4. Нажмите **Добавить подсеть**.

5. Выберите приватную подсеть или подсеть глобального роутера.

6. Введите IP-адрес роутера. IP-адрес облачного роутера должен совпадать с шлюзом по умолчанию приватной подсети. Посмотреть шлюз по умолчанию в приватной подсети можно на вкладке **Приватные сети** → страница сети → вкладка **Подсети** → карточка подсети → блок **Автоматические сетевые настройки** → поле **Шлюз подсети**.

   Если вы подключаете подсеть глобального роутера, IP-адрес облачного роутера должен совпадать со шлюзом по умолчанию подсети глобального роутера и отличаться от IP-адреса глобального роутера, IP-адресов устройств в сети и служебных адресов `.253` и `.254`.

7. Нажмите **Добавить подсеть**.

Отключить подсеть от облачного роутера

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. Откройте карточку роутера.
4. В меню ⋮ приватной подсети выберите **Удалить порт**.
5. Нажмите **Удалить**.

Подключить облачный роутер к внешней сети

Чтобы настроить доступ в интернет для устройств в приватной подсети, подсеть должна быть подключена к облачному роутеру с выходом во внешнюю сеть (`external-network`). При подключении роутера к внешней сети для него будет выделен внешний IP-адрес, через который роутер будет выполнять функцию 1:1 NAT.
Если роутер объединяет несколько приватных подсетей, устройства во всех подсетях будут иметь доступ в интернет.
Чтобы настроить доступ из интернета для устройств в приватных подсетях с помощью облачного роутера, используйте инструкцию Настроить доступ в интернет и из интернета.

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. В меню ⋮ облачного роутера выберите **Подключить к внешней сети**.

Отключить облачный роутер от внешней сети

Если вы отключите облачный роутер от внешней сети, его внешний IP-адрес вернется в пул адресов. После повторного подключения IP-адрес изменится.

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.

2. Откройте вкладку **Облачные роутеры**.
3. В меню ⁝ облачного роутера выберите **Отключить от внешней сети**.

Назначить файрвол на порт облачного роутера

Входящий и исходящий трафик, который не разрешен в правилах облачного файрвола, будет запрещен на порте облачного роутера. На роутере прервутся активные сессии, которые нельзя устанавливать по новым правилам.
На один порт роутера нельзя назначить более одного файрвола.

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. Откройте карточку облачного роутера.
4. В строке приватной подсети, для которой нужно настроить фильтрацию трафика, в столбце **Файрвол** нажмите **Подключить**.
5. Выберите файрвол.
6. Нажмите **Назначить**.

Отключить файрвол от порта облачного роутера

Правила облачного файрвола перестанут действовать — весь входящий и исходящий трафик, который проходит через порт облачного роутера, будет разрешен.

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. Откройте карточку роутера.
4. В меню ⁝ приватной подсети, для которой была настроена фильтрация трафика, выберите **Отключить порт от порта**.
5. Нажмите **Отключить**.

Включить облачный роутер

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. В карточке облачного роутера включите роутер.

Выключить облачный роутер

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. В карточке облачного роутера отключите роутер.

Удалить облачный роутер

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. Если к роутеру подключены подсети, удалите порты роутера в подсетях. Для этого откройте карточку роутера и в меню ⁝ подсети выберите **Удалить порт**.

4. В меню ⋮ роутера выберите **Удалить роутер**.
5. Нажмите **Удалить**.

Публичные IP-адреса

Публичные статические IP-адреса можно подключать к устройствам, чтобы настроить к ним доступ из интернета: к облачному серверу, балансировщику нагрузки, кластеру облачных баз данных.
Для доступа устройство должно находиться в приватной подсети, подключенной к облачному роутеру с выходом во внешнюю сеть, — подробнее в инструкции Подготовить приватную подсеть для подключения публичного IP-адреса. Публичный IP-адрес ассоциируется с приватным IP-адресом устройства, а входящий трафик обрабатывается облачным роутером — он выполняет функцию 1:1 NAT через внешний IP-адрес, который выделяется при подключении роутера к внешней сети. Входящий трафик можно отфильтровать с помощью облачного файрвола.
При создании публичный IP-адрес выделяется из пула адресов автоматически, его нельзя выбрать. Адрес является плавающим (в API — Floating IP), так как его можно быстро переключать между устройствами в приватных подсетях. При переключении адрес не меняется и не удаляется.
Публичный IP-адрес можно использовать только внутри одного проекта и одного пула.
Для публичных IP-адресов есть ограничения на объем трафика — пропускная способность. Ее можно посмотреть в таблице Пропускная способность.
Работать с публичными IP-адресами можно в панели управления, с помощью OpenStack CLI или Terraform.

Создать публичный IP-адрес

Если вы создаете первый публичный IP-адрес внутри проекта и пула, автоматически создастся приватная сеть `nat` и облачный роутер `router-nat`.

1. В панели управления перейдите в раздел **Облачная платформа → Сеть**.
2. Откройте вкладку **Публичные IP-адреса**.
3. Нажмите **Создать IP-адрес**.
4. Выберите пул, в котором будет создан публичный IP-адрес.
5. Укажите количество публичных IP-адресов.
6. Нажмите **Создать**.

Подготовить приватную подсеть для подключения публичного IP-адреса

Чтобы настроить доступ в интернет и из интернета через публичный IP-адрес, нужно подключить его к устройству.
Устройство должно находиться в приватной подсети или подсети глобального роутера, которая соответствует требованиям:

- подсеть должна быть подключена к облачному роутеру, подключенному к внешней сети. Если облачный роутер подключен к внешней сети, он выполняет функцию 1:1 NAT для доступа из приватной сети в интернет через внешний адрес роутера и для доступа к устройству в приватной подсети из интернета по публичному IP-адресу;
- приватный IP-адрес облачного роутера должен совпадать с шлюзом по умолчанию в подсети.

Если подсеть не соответствует требованиям, подготовьте ее к подключению публичного IP-адреса:

1. Создайте облачный роутер с подключением к внешней сети.
2. Подключите приватную подсеть к облачному роутеру.

1. Создать облачный роутер с подключением к внешней сети

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. Нажмите **Создать роутер**.
4. Выберите пул, в котором будет создан облачный роутер.
5. Введите имя роутера.
6. Отметьте чекбокс **Подключить роутер к внешней сети** — для роутера будет выделен внешний IP-адрес.
7. Нажмите **Создать**.

2. Подключить подсеть к облачному роутеру

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Облачные роутеры**.
3. Откройте карточку роутера.
4. Нажмите **Добавить подсеть**.
5. Выберите приватную подсеть или подсеть глобального роутера.
6. Введите IP-адрес роутера. IP-адрес облачного роутера должен совпадать с шлюзом по умолчанию приватной подсети. Посмотреть шлюз по умолчанию в приватной подсети можно на вкладке **Приватные сети** → страница сети → вкладка **Подсети** → карточка подсети → блок **Автоматические сетевые настройки** → поле **Шлюз подсети**.

   Если вы подключаете подсеть глобального роутера, IP-адрес облачного роутера должен совпадать со шлюзом по умолчанию подсети глобального роутера и отличаться от IP-адреса глобального роутера, IP-адресов устройств в сети и служебных адресов `.253` и `.254`.
7. Нажмите **Добавить подсеть**.

Подключить публичный IP-адрес к облачному серверу

Публичный IP-адрес можно подключить при создании облачного сервера или к уже созданному серверу.

1. Убедитесь, что облачный сервер находится в подсети, которая соответствует требованиям. Для подготовки подсети используйте инструкцию Подготовить приватную подсеть для подключения публичного IP-адреса. Подсети сервера можно посмотреть в панели управления в разделе **Облачная платформа** → **Серверы** → страница сервера → вкладка **Порты**.
2. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
3. Откройте вкладку **Серверы** → страницу сервера.
4. Откройте вкладку **Порты**.
5. В столбце **Публичный IP** нажмите **Подключить**.
6. Выберите публичный IP-адрес.

Отключить публичный IP-адрес от облачного сервера

1. В панели управления перейдите в раздел **Облачная платформа** → **Серверы**.
2. Откройте вкладку **Серверы** → страницу сервера.
3. Откройте вкладку **Порты**.
4. В столбце **Публичный IP** в меню ⋮ выберите **Отключить публичный IP**.
5. Нажмите **Отключить**.

Подключить публичный IP-адрес к балансировщику нагрузки

Публичный IP-адрес можно подключить при создании балансировщика нагрузки или к уже созданному балансировщику.

1. Убедитесь, что балансировщик нагрузки находится в подсети, которая соответствует требованиям. Для подготовки подсети используйте инструкцию Подготовить приватную подсеть для подключения публичного IP-адреса. Подсети балансировщика можно посмотреть в панели управления в разделе **Облачная платформа** → **Балансировщики** → вкладка **Балансировщики** → страница балансировщика → поле **Сеть**.
2. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
3. Откройте вкладку **Балансировщики**.
4. В карточке балансировщика нажмите **Подключить публичный IP**.
5. Выберите публичный IP-адрес.
6. Нажмите **Подключить**.

Отключить публичный IP-адрес от балансировщика нагрузки

1. В панели управления перейдите в раздел **Облачная платформа** → **Балансировщики**.
2. Откройте вкладку **Балансировщики**.
3. В карточке балансировщика у публичного IP-адреса нажмите □.
4. Выберите **Отключить публичный IP-адрес**.
5. Нажмите **Сохранить**.

Подключить публичный IP-адрес к кластеру облачных баз данных

Публичный IP-адрес можно подключить при создании кластера баз данных (пример для PostgreSQL) или к уже созданному кластеру.

1. Убедитесь, что кластер облачных баз данных находится в подсети, которая соответствует требованиям. Для подготовки подсети используйте инструкцию Подготовить приватную подсеть для подключения публичного IP-адреса. Подсети кластера можно посмотреть в панели управления в разделе **Облачная платформа** → **Базы данных** → страница кластера → вкладка **Настройки** → поле **Сеть кластера**.
2. В панели управления перейдите в раздел **Облачная платформа** → **Базы данных**.
3. Откройте страницу кластера баз данных → вкладка **Настройки**.
4. В блоке **Адреса и статусы нод** откройте вкладку **Публичные IP-адреса**.
5. В строке с нужной нодой нажмите .
6. Выберите **Новый публичный IP-адрес**.
7. Нажмите ✓.

Отключить публичный IP-адрес от кластера облачных баз данных

1. В панели управления перейдите в раздел **Облачная платформа** → **Базы данных**.
2. Откройте страницу кластера баз данных → вкладка **Настройки**.
3. В блоке **Адреса и статусы нод** откройте вкладку **Публичные IP-адреса**.
4. В строке с нужной нодой нажмите .
5. Выберите **Без публичного IP-адреса**.
6. Нажмите ✓.

Удалить публичный IP-адрес

После удаления публичный IP-адрес вернется в пул публичных адресов.

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Публичные IP-адреса**.
3. В карточке публичного IP-адреса нажмите 🗑️.
4. Введите IP-адрес для подтверждения удаления.
5. Нажмите **Удалить**.

Публичные подсети

Публичная подсеть — это диапазон публичных статических IP-адресов, ограниченный размером префикса (маски). Все устройства в публичной подсети имеют публичный IP-адрес и доступ в интернет и из интернета. Настроить доступ через публичную подсеть можно для облачного сервера, облачного балансировщика нагрузки и кластера облачных баз данных — подробнее в инструкции Настроить доступ в интернет и из интернета.
IP-адреса из публичной подсети не обрабатываются облачным роутером с помощью 1:1 NAT, а подключаются напрямую к устройствам: облачному серверу, облачному балансировщику нагрузки, кластеру облачных баз данных. Из-за отсутствия NAT такой вид подключения устройств к интернету более отказоустойчивый и быстрый, но менее безопасный, чем подключение через публичный IP-адрес.
Устройства в публичной подсети взаимодействуют друг с другом через публичные интерфейсы.
Публичную подсеть можно использовать только внутри одного проекта и одного пула.
Внутри публичных подсетей есть ограничения на объем трафика — пропускная способность. Ее можно посмотреть в таблице Пропускная способность.
Работать с публичными подсетями можно в панели управления или Terraform.

Размеры публичных подсетей

Доступны публичные подсети размером от /29 (пять свободных адресов IPv4) до /24 (253 свободных адреса IPv4). В каждой публичной подсети резервируется три служебных IP-адреса:

- первый IP-адрес — адрес сети;
- второй IP-адрес — адрес шлюза;
- последний IP-адрес — широковещательный адрес.

Остальные IP-адреса можно назначить на устройства.
Пример для подсети `192.0.2.0/29` — доступны пять адресов:

- 192.0.2.0 — адрес сети;
- 192.0.2.1 — адрес шлюза;
- 192.0.2.2 — можно использовать;
- 192.0.2.3 — можно использовать;
- 192.0.2.4 — можно использовать;
- 192.0.2.5 — можно использовать;
- 192.0.2.6 — можно использовать;
- 192.0.2.7 — широковещательный адрес.

Если в публичной подсети закончились свободные IP-адреса, можно создать новую публичную подсеть.

Автоматические настройки публичной подсети

В публичных подсетях указываются настройки по умолчанию: шлюз по умолчанию и DNS-серверы. Настройки применяются к устройствам в подсети автоматически.

Шлюз по умолчанию

При создании публичной подсети для шлюза по умолчанию резервируется второй IP-адрес. Шлюз по умолчанию в публичной подсети нельзя изменить.

DNS-серверы

При создании публичной подсети на устройствах в подсети автоматически прописываются DNS-серверы Selectel. DNS-серверы можно изменить при создании подсети или изменить после создания.

Статические маршруты

По умолчанию в подсетях не указаны статические маршруты. Для публичных подсетей можно настроить статические маршруты.

Создать публичную подсеть

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Публичные сети**.
3. Нажмите **Создать подсеть**.
4. Выберите пул, в котором будет создана публичная подсеть.
5. Выберите размер подсети — диапазон IP-адресов, доступных в подсети.
6. Опционально: чтобы изменить DNS-серверы, нажмите . Введите от одного до трех значений. Нажмите ✓.
7. Нажмите **Создать**.

Настроить доступ к публичной подсети в разных проектах

По умолчанию публичную подсеть можно использовать только внутри одного проекта и одного пула. Вы можете настроить общий доступ к публичной подсети в разных проектах внутри одного аккаунта. Подсеть так же будет доступна только внутри одного пула.
У публичной подсети появится тег `Кросспроектная`. Управлять подсетью можно будет только в проекте, в котором находится подсеть.

1. В панели управления перейдите в раздел **Облачная платформа**.
2. Скопируйте ID проекта-получателя, с которым нужно поделиться подсетью. Откройте меню проектов (название текущего проекта) и в строке нужного проекта нажмите .
3. Убедитесь, что вы находитесь в проекте, в котором находится подсеть. Откройте меню проектов (название текущего проекта) и выберите исходный проект.
4. Перейдите в раздел **Облачная платформа** → **Сеть**.
5. Откройте вкладку **Публичные сети**.
6. Откройте карточку сети → вкладка **Проекты**.
7. Нажмите **Добавить проект**.
8. Вставьте ID проекта-получателя, который вы скопировали на шаге 2.
9. Нажмите ✓.

Изменить DNS-серверы в публичной подсети

При создании публичной подсети на устройствах в подсети автоматически прописываются рекурсивные DNS-серверы Selectel. DNS-серверы можно изменить при создании публичной подсети или для существующей публичной подсети.

1. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
2. Откройте вкладку **Публичные сети**.
3. Откройте карточку публичной подсети → вкладка **Подсети**.
4. В строке подсети в столбце **DNS-серверы** нажмите .
5. Введите от одного до трех значений.
6. Нажмите ✓.

Удалить публичную подсеть

1. Панель управления
2. В панели управления перейдите в раздел **Облачная платформа** → **Сеть**.
3. Откройте вкладку **Публичные сети**.
4. В меню ⋮ публичной подсети выберите **Удалить подсеть**.
5. Введите адрес подсети для подтверждения удаления.
6. Нажмите **Удалить**.

Файловое хранилище

Общая информация

Эластичное файловое сетевое хранилище Selectel — это отказоустойчивая масштабируемая файловая система для хранения данных. Его можно подключить:

- к облачным серверам;
- выделенным серверам (кроме линейки Chipcore Line);
- нодам кластеров Managed Kubernetes.

Эластичное файловое хранилище можно подключить к нескольким продуктам одновременно, в том числе в разных пулах. Например, можно подключить хранилище к выделенному серверу в пуле SPB-1 и облачному серверу в сегменте пула ru-7a — серверы смогут одновременно использовать хранилище.

Эластичное файловое хранилище работает на базе сетевых дисков облачной платформы с трехкратной репликацией томов диска.

Работать с файловым хранилищем можно в панели управления, через OpenStack CLI или Terraform.

В продукте поддерживаются типы и роли пользователей, проекты и лимиты проекта и квоты.

Протоколы

Поддерживаются протоколы NFSv4 и CIFS SMBv3.

Ограничения

Минимальный размер эластичного файлового хранилища — 50 ГБ, максимальный — 50 ТБ.

Типы эластичного файлового хранилища

- HDD Базовое — подходит для хранения больших объемов данных, которые не нужно часто читать или перезаписывать: резервных копий, архивов, документов;
- SSD Универсальное — можно использовать как основную инфраструктуру для хранения данных, если невозможно подключить диск, а также для хранения наборов данных и моделей в кластерах машинного обучения и хранения «сырых» данных для высокопроизводительных вычислений. Можно использовать в Kubernetes как постоянный том (Persistent Volume) с режимом доступа ReadWriteMany (монтирование тома к нескольким нодам);
- SSD Быстрое — подходит для нагрузок, при которых нужна повышенная производительность ввода и вывода данных, а также для хранения наборов данных и моделей в кластерах машинного обучения и хранения «сырых» данных для высокопроизводительных вычислений. Можно использовать в Kubernetes как

постоянный том (Persistent Volume) с режимом доступа ReadWriteMany (монтирование тома к нескольким нодам).

Типы эластичного файлового хранилища отличаются значениями пропускной способности и количеством операций на чтение и запись. Подробнее в таблице Лимиты файлового хранилища.

В разных сегментах пула доступны разные типы эластичного файлового хранилища. Посмотреть доступность типов можно в матрице доступности Эластичное файловое хранилище.

Лимиты эластичного файлового хранилища

Значения пропускной способности и лимиты на чтение и запись в IOPS зависят от типа эластичного файлового хранилища.

Эластичные файловые хранилища одного типа в разных сегментах пула могут иметь разные лимиты. Например, если два хранилища с типом SSD Универсальное находятся в разных сегментах (первое в ru-1c, второе — в ru-8a), их лимиты будут различаться.

	HDD Базовое (все доступные сегменты пула)	**SSD Универсальное**	**SSD Быстрое**
Пропускная способность (чтение, блоки 4 МБ)	40 МБ/с (для NFSv4) 100 МБ/с (для CIFS SMBv3)	200 МБ/с	300 МБ/с
Пропускная способность (запись, блоки 4 МБ)	100 МБ/с	200 МБ/с	500 МБ/с
Количество операций (чтение, блоки 4 КБ)	320 IOPS	7000 IOPS	25000 IOPS

Количество операций (запись, блоки 4 КБ)	120 IOPS	4000 IOPS	15000 IOPS

Вы можете протестировать производительность эластичного файлового хранилища.

Модель оплаты и цены файлового хранилища

Если вы создали эластичное файловое хранилище до 13 июня 2023 года через техническую поддержку, оно предоставляется по разовой оплате и оплачивается каждый месяц. В этой инструкции описана модель оплаты и цены эластичного файлового хранилища, которое создано в панели управления.

Баланс

Для оплаты ресурсов облачной платформы в зависимости от типа баланса в аккаунте используется единый баланс или баланс облачной платформы.

Оплатить ресурсы можно разными типами средств: основными средствами, бонусами или ВК бонусами.

Перед оплатой пополните баланс.

Модель оплаты

В облачной платформе используется модель оплаты pay-as-you-go. С баланса каждый час списываются средства за предыдущий час использования ресурсов облачной платформы.

Все созданные ресурсы оплачиваются, даже если они выключены.

Подробнее об оплате в документе Условия использования отдельных сервисов: группа услуг Облачная платформа.

Блокировка ресурсов, если на балансе недостаточно средств

Если на момент списания на балансе будет недостаточно средств для оплаты, то все ресурсы облачной платформы автоматически заблокируются — при этом за них продолжит начисляться плата.

Чтобы восстановить доступ к ресурсам, нужно пополнить баланс на сумму долга в течение 14 дней после блокировки. Долг за ресурсы, которые тарифицировались в период блокировки, автоматически погасится. Проекты не блокируются — можно удалить проект целиком или ресурсы через API.

Если в течение 14 дней после блокировки не пополнить баланс на сумму долга, все ресурсы удалятся. Проекты при этом не удаляются.

Чтобы не пропускать пополнения баланса, вы можете настроить уведомления о состоянии баланса.

Внутренний трафик

Внутренний трафик — это входящий и исходящий трафик между публичным адресом объекта облачной платформы и публичным адресом другой услуги Selectel, например Выделенный сервер или Объектное хранилище.

Трафик между проектами и пулами облачной платформы Selectel тоже относится к внутреннему.

Со стороны облачной платформы трафик (входящий и исходящий) до любых других услуг Selectel не оплачивается.

Посмотреть потребление

Посмотреть текущую стоимость всей облачной инфраструктуры, потребление и оплату инфраструктуры и внешнего трафика можно в панели управления в разделе **Облачная платформа** → **Потребление платформы**.

Текущая стоимость

Текущая стоимость — это количество денег, которое потребляет текущая конфигурация облачной инфраструктуры за определенное время.

Текущую стоимость можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Текущая стоимость**.

Можно посмотреть текущую стоимость определенных проектов, ресурсов и пулов за час, день или месяц.

Данные о стоимости инфраструктуры обновляются каждый час. В панели управления они отображаются на 5–35 минут позже реального изменения инфраструктуры и ее стоимости. Недавно удаленные ресурсы могут продолжать отображаться в панели управления до следующего обновления данных. При этом ресурсы перестают тарифицироваться со следующего часа после удаления.

Графики потребления и оплаты

Графики потребления и оплаты инфраструктуры можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **График расходов** → вкладки **Потреблено** и **Оплачено**.

Можно посмотреть потребление определенных проектов, объектов, ресурсов, регионов и пулов. Графики потребления и оплаты можно посмотреть за определенный период времени или отсортировать по дням, неделям, месяцам, годам.

Чтобы выгрузить детализацию потребления и оплаты в формате `.csv`, нажмите **Скачать CSV** и выберите, как будут сгруппированы строки в выгрузке (по часам, дням, неделям, месяцам, годам).

Все блокировки ресурсов отображаются на графиках потребления и графиках оплаты.

Трафик

Потребление внешнего трафика за текущий месяц можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Внешний трафик**.

Чтобы выгрузить детализацию потребления внешнего и внутреннего трафика за каждый час по всем публичным адресам аккаунта в формате `.csv`, выберите период и нажмите **Скачать CSV**. Можно выгрузить детализацию только за последние три месяца.

Цены

Цены на ресурсы можно посмотреть на selectel.ru. Цены в пулах могут различаться.

Отчетные документы

После оплаты можно получить отчетные документы.

Создать эластичное файловое хранилище

1. В панели управления перейдите в раздел **Облачная платформа → Файловое хранилище**.

2. Нажмите **Создать хранилище**.

3. Введите новое имя хранилища или оставьте имя, которое создано автоматически.

4. Выберите регион и сегмент пула, в котором будет создано хранилище.

   Если с помощью эластичного файлового хранилища нужно увеличить дисковое пространство, выберите сегмент пула из пула, в котором расположен облачный сервер или кластер Managed Kubernetes. Если вы планируете использовать хранилище для хранения бэкапов, мы рекомендуем выбрать сегмент пула из другой зоны доступности или региона для повышения отказоустойчивости.

5. Выберите приватную подсеть, в которой будет находиться хранилище. Тип подсети зависит от того, к чему нужно подключить хранилище:

   - облачная приватная подсеть — хранилище будет доступно для облачных серверов и кластеров Managed Kubernetes только в том пуле, который вы выбрали на предыдущем шаге. Для подключения хранилища нужно будет только примонтировать его;
   - подсеть глобального роутера — хранилище будет доступно для выделенных серверов, а также облачных серверов и кластеров Managed Kubernetes, которые находятся в других пулах. Для подключения хранилища нужно настроить сетевую связность между сервером или кластером и хранилищем через глобальный роутер. Посмотрите примеры настройки сетевой связности в инструкциях Подключить файловое хранилище к выделенному серверу, Подключить файловое хранилище к облачному серверу в другом пуле, Подключить файловое хранилище к кластеру Managed Kubernetes в другом пуле.
6. После создания хранилища подсеть нельзя будет изменить.

7. Введите приватный IP-адрес хранилища или оставьте первый доступный адрес из подсети, который назначается по умолчанию. После создания хранилища IP-адрес нельзя будет изменить.

8. Выберите тип эластичного файлового хранилища:

   - HDD Базовое;
   - SSD Универсальное;
   - SSD Быстрое.
9. Типы эластичного файлового хранилища отличаются значениями пропускной способности и количеством операций на чтение и запись, подробнее в таблице Лимиты эластичного файлового хранилища.

После создания тип хранилища нельзя будет изменить.

10. Укажите размер хранилища: от 50 ГБ до 50 ТБ. После создания можно будет увеличить эластичное файловое хранилище, но нельзя уменьшить.

11. Выберите протокол:

    - NFSv4 — для подключения хранилища к серверам с операционной системой Linux и другими Unix-системами;
    - CIFS SMBv3 — для подключения хранилища к серверам с операционной системой Windows.

12. После создания хранилища протокол нельзя будет изменить.

13. Настройте правила доступа к эластичному файловому хранилищу:

    - доступно всем — хранилище будет доступно для любого IP-адреса приватной подсети, в которой оно создается;
    - доступ ограничен — хранилище будет доступно только для определенных IP-адресов или приватных подсетей. Если создать эластичное файловое хранилище без правил, доступ будет ограничен для всех IP-адресов. Чтобы открыть доступ, нажмите **Добавить правило**, введите IP-адрес или CIDR приватной подсети, выберите уровень доступа (только для протокола NFSv4) и введите комментарий. Чтобы добавить дополнительные правила, нажмите **Добавить правило**.

14. После создания хранилища можно изменить правила доступа, для этого можно настроить новые правила доступа.

15. Проверьте цену эластичного файлового хранилища.

16. Нажмите **Создать**.

Подключить эластичное эластичное эластичное файловое хранилище

Для подключения эластичного файлового хранилища используйте инструкции:

- **Подключить эластичное файловое хранилище к выделенному серверу**
- **Подключить эластичное файловое хранилище к облачному серверу в другом пуле**
- **Подключить эластичное файловое хранилище к облачному серверу в одном пуле**
- **Подключить эластичное файловое хранилище к Managed Kubernetes в другом пуле**
- **Подключить эластичное файловое хранилище к Managed Kubernetes в одном пуле**

Работа с файловым хранилищем

Примонтировать эластичное файловое хранилище

Эластичное файловое хранилище можно примонтировать:

- к выделенному или облачному серверу;
- кластеру Managed Kubernetes.

Настроить доступ к эластичному файловому хранилищу определенным IP-адресам или подсетям

К эластичному файловому хранилищу можно настроить доступ, добавив правила. Можно открыть доступ к хранилищу:

- всем IP-адресам приватной подсети, в которой находится хранилище;
- определенным IP-адресам;
- другим приватным подсетям.

Для каждого правила можно выбрать уровень доступа.

Настроить правила доступа можно при создании эластичного файлового хранилища или у существующего эластичного файлового хранилища — добавить правила или удалить правила.

Уровни доступа

В зависимости от протокола эластичного файлового хранилища можно назначить уровень доступа к хранилищу:

- для CIFS SMBv3 — чтение и запись (`rw`);
- для NFSv4 — только чтение (`ro`); чтение и запись (`rw`).

Добавить правило

Новый список правил доступа для файловых хранилищ с протоколом NFSv4 применяется до 15 минут после добавления или удаления правил.

Правила применяются по порядку в списке — сверху вниз:

- правило доступа к хранилищу с любого IP-адреса приватной подсети (`0.0.0.0/0`);
- правила доступа из приватных подсетей (например, `192.168.0.0/29`);
- правила доступа с IP-адресов (например, `192.168.0.10`).

Например, если добавлены правила `0.0.0.0/0`, `192.168.0.0/29`, `192.168.0.1`, то к хранилищу будет открыт доступ с любого IP-адреса приватной подсети.

Чтобы добавить правило:

1. В панели управления перейдите в раздел **Облачная платформа** → **Файловое хранилище**.
2. Откройте страницу эластичного файлового хранилища → вкладка **Правила доступа**.
3. Нажмите **Добавить правило**.
4. Введите IP-адрес или CIDR приватной подсети.
5. Выберите уровень доступа.
6. Опционально: введите комментарий для правила.
7. Нажмите **Сохранить**.
8. Опционально: чтобы добавить дополнительное правило, нажмите **+ Добавить правило**.

Удалить правило

Новый список правил доступа для файловых хранилищ с протоколом NFSv4 применяется до 15 минут после добавления или удаления правил.

1. В панели управления перейдите в раздел **Облачная платформа** → **Файловое хранилище**.
2. Откройте страницу эластичного файлового хранилища → вкладка **Правила доступа**.
3. В строке правила нажмите 🗑️.
4. Нажмите **Удалить**.

Управлять правами доступа в эластичном файловом хранилище на уровне файловой системы

В эластичном файловом хранилище с протоколом NFSv4 можно управлять правами доступа к файлам и папкам на уровне файловой системы.

Принцип работы

Файлы и папки в эластичном файловом хранилище с протоколом NFSv4 поддерживают стандартное разграничение прав доступа как в Unix-системах. Доступ на чтение, запись и выполнение файлов реализован через Identity Mapping (IDM) — права доступа проверяются на основе ID пользователя и ID группы пользователей.

Группа пользователей — это пользователи с одинаковыми правами доступа. Группы делятся на два типа:

- первичная группа (Primary Group) — группа, которую операционная система присваивает пользователю;
- вторичная группа (Secondary Group) — одна или несколько групп, к которым также принадлежит пользователь.

Каждого пользователя можно добавить максимум в 16 групп: в одну первичную и 15 вторичных групп.

По умолчанию права на чтение, запись и выполнение файлов есть только у пользователя `root`. У остальных пользователей есть права только на чтение. От имени `root` можно настроить права доступа к папкам и файлам для пользователей и для групп пользователей.

Формат прав доступа

Пример прав доступа:

```
Unset
drwxrwxrwx 3 root root   21 Jun 13 14:00 .
drwxr-xr-x 4 root root 4096 Jun 13 13:44 ..
drwxr-xr-x 2 root root    6 Jun 13 14:00 directory
-rw-rw-r-- 1 first first  0 Jun 13 09:45 file.txt
```

Здесь:

- первый символ:
  - `d` — флаг директории;
  - `-` — флаг файла;
- тройки символов вида `rwx`:
  - первая тройка символов вида `rwx` — права пользователя;
  - вторая тройка символов вида `rwx` — права группы;
  - третья тройка символов вида `rwx`— права всех остальных, кто не является пользователем или не входит в группу;
  - `r` — права на чтение (read);
  - `w` — права на запись (write);
  - `x` — права на выполнение (execute);
- первый столбец с именами — имена пользователей, которые являются владельцами папки или файла;
- второй столбец с именами — имена групп, которые являются владельцами папки или файла;
- последний столбец — имена файлов или директорий.

Настроить права доступа для пользователя

Пользователь `root` может создавать пользователей и выдавать им права на папки. Если создать пользователя, папку и назначить пользователя владельцем папки, то только у этого пользователя будут полные права на чтение, запись и выполнение файлов в папке.

1. Примонтируйте эластичное файловое хранилище.
2. Создайте пользователя.
3. Назначьте пользователя владельцем папки.
4. Проверьте права пользователя.

Настроить права доступа для группы

Пользователь `root` может создавать вторичные группы пользователей (Secondary Groups) и выдавать группам права на папки. Все пользователи в группе будут обладать одинаковыми правами доступа. Любой пользователь из группы сможет создавать файлы, а также изменять файлы, которые создал другой пользователь группы.

Если вы создали эластичное файловое хранилище до 9 августа 2024 года, для включения опции разграничения прав на вторичные группы создайте тикет. После включения опции нужно будет отмонтировать и примонтировать его заново.

1. Примонтируйте эластичное файловое хранилище.
2. Создайте вторичную группу пользователей.
3. Назначьте вторичную группу пользователей владельцем папки.
4. Проверьте права вторичной группы пользователей.

Увеличить эластичное файловое хранилище

После увеличения размера эластичного файлового хранилища его нельзя будет уменьшить.

Если вы создали эластичное файловое хранилище до 13 июня 2023 года через техническую поддержку, для увеличения хранилища создайте тикет и укажите в нем новый размер хранилища. После увеличения хранилища изменится тариф: мы вернем средства за неиспользованные дни предыдущего тарифа и спишем оплату за новый. В этой инструкции описано увеличение эластичного файлового хранилища, которое создано в панели управления.

1. В панели управления перейдите в раздел **Облачная платформа** → **Файловое хранилище**.
2. Откройте страницу эластичного файлового хранилища → вкладка **Настройки**.
3. В поле **Размер** нажмите **Изменить**.
4. Нажмите ✓.

Удалить эластичное файловое хранилище

После удаления эластичного файлового хранилища данные нельзя будет восстановить.

Если вы создали эластичное файловое хранилище до 13 июня 2023 года через техническую поддержку, для удаления хранилища создайте тикет. Если вы ранее оплатили месяц использования хранилища, после удаления средства не вернутся. В этой инструкции описано удаление эластичного файлового хранилища, которое создано в панели управления.

1. Отмонтируйте эластичное файловое хранилище.
2. В панели управления перейдите в раздел **Облачная платформа** → **Файловое хранилище**.
3. В строке эластичного файлового хранилища нажмите 🗑️.

Managed Kubernetes

Общая информация

Managed Kubernetes от Selectel упрощает процесс развертывания, масштабирования и обслуживания контейнерной инфраструктуры Kubernetes. Selectel отвечает за обновление версий, безопасность и работоспособность Control Plane Kubernetes.

В продукте поддерживаются типы и роли пользователей, проекты и лимиты проекта и квоты.

Версии

В кластерах Managed Kubernetes на облачных серверах поддерживаются версии 1.28.x, 1.29.x, 1.30.x

В кластерах Bare-metal Kubernetes на выделенных серверах поддерживается только версия 1.28.x

Как работает Managed Kubernetes

Managed Kubernetes может работать:

- на облачных серверах — используются ресурсы облачной платформы;
- выделенных серверах (Bare-metal Kubernetes) — используются выделенные серверы, сети выделенных серверов и ресурсы облачной платформы (балансировщики нагрузки, публичные подсети, публичные IP-адреса).

Подробнее об используемых ресурсах в инструкции Проекты.

В качестве среды исполнения контейнеров (CRI) используется containerd. В качестве CNI в кластерах Managed Kubernetes используется Calico.

С кластером Managed Kubernetes можно работать в панели управления и через API Managed Kubernetes. С кластером на облачном серевере также можно работать через Terraform.

Состав кластера

Кластеры Managed Kubernetes состоят:

- из мастер-нод — содержат управляющие компоненты кластера, Control Plane. Количество мастер-нод зависит от типа кластера. Мастер-ноды не отображаются в панели управления, за них отвечает Selectel;

- групп рабочих нод — содержат контейнеры пользовательских приложений. Рабочие ноды отображаются в панели управления, за них отвечает пользователь.

Подробнее в разделе Работа с группами нод.

Типы кластера

От типа кластера зависит его отказоустойчивость. Selectel предоставляет два типа кластеров Managed Kubernetes:

- отказоустойчивый — Control Plane размещен на трех мастер-нодах, которые запускаются на разных хостах в сегментах одного пула. Если одна из трех мастер-нод недоступна, Control Plane продолжит работать;
- базовый — Control Plane размещен на одной мастер-ноде в одном сегменте пула. Если мастер-нода недоступна, Control Plane не будет работать.

Выбрать тип кластера можно только при создании кластера. После создания кластера тип кластера нельзя изменить.

Ограничения

Облачный сервер

Максимальное количество отказоустойчивых кластеров Kubernetes в одном пуле для одного проекта	10
Максимальное количество базовых кластеров Kubernetes в одном пуле для одного проекта	10
Максимальное количество групп нод в одном пуле для одного проекта	100
Максимальное количество нод в одной группе нод	15
Максимальное количество vCPU ноды	32*
Максимальное количество RAM ноды	256* ГБ
Максимальный размер загрузочного диска ноды	1,2 ТБ
Максимальное количество подов на одной ноде	100
Максимальное количество PV на одной ноде	256
Минимальный размер одного PV	1 ГБ

*Вы можете создать ноды с бóльшим количеством vCPU и RAM — используйте фиксированные конфигурации облачных серверов.

Bare-metal Kubernetes

- максимальное количество отказоустойчивых кластеров Kubernetes в одном пуле для одного проекта — 10;
- максимальное количество базовых кластеров Kubernetes в одном пуле для одного проекта — 10;
- максимальное количество групп нод в кластере — 1;
- максимальное количество нод в одной группе нод — 20;
- не поддерживается изменение количества нод в группе;
- группу нод на выделенных серверах можно добавить только в новые кластеры;
- группа нод на выделенных серверах должна находиться в одной зоне доступности с мастер-нодами;
- доступна только версия Kubernetes 1.28.x. Обновление версий Kubernetes не поддерживается;
- не поддерживается автоматизация: автообновление патч-версий, автомасштабирование и автовосстановление;
- не поддерживается добавление, изменение и удаление меток и тейнтов после создания кластера;
- не поддерживается подключение постоянных томов (PV) на базе сетевых дисков облачной платформы;
- не поддерживается создание кластеров Bare-metal Kubernetes с GPU и Intel® SGX.

Зоны ответственности

Selectel обеспечивает

- создание и доступность мастер-нод;
- создание рабочих нод;
- обновление версий кластера Managed Kubernetes;
- мониторинг мастер-нод;
- возможность автомасштабирования нод;
- возможность автовосстановления нод;
- безопасность хранения данных в соответствии с требованиями 152-ФЗ;
- интеграцию с сервисами Selectel;
- техническую поддержку.

Selectel не несет ответственность

- за управление кластером Managed Kubernetes;
- управление рабочими нодами;
- создание приложения;
- инициирование масштабирования и обновления.

Если вам нужна помощь с администрированием кластеров Managed Kubernetes, закажите услуги администрирования сервисов.

Модель оплаты и цены Managed Kubernetes

Managed Kubernetes может работать:

- на облачных серверах — оплачиваются ресурсы облачной платформы;
- или выделенных серверах (Bare-metal Kubernetes) — оплачиваются выделенные серверы, сети выделенных серверов и ресурсы облачной платформы (балансировщики нагрузки, публичные подсети, публичные IP-адреса).

Баланс

Ресурсы облачной платформы

Для оплаты ресурсов облачной платформы в зависимости от типа баланса в аккаунте используется единый баланс или баланс облачной платформы.

Оплатить ресурсы можно разными типами средств: основными средствами, бонусами или ВК бонусами.

Перед оплатой пополните баланс.

Ресурсы Bare-metal Kubernetes

Для оплаты ресурсов выделенного сервера в зависимости от типа баланса в аккаунте используется единый баланс или основной баланс.

Оплатить ресурсы выделенного сервера можно разными типами средств: основными средствами или бонусами и ВК бонусами.

Перед оплатой пополните баланс.

Модель оплаты

Ресурсы облачной платформы

В облачной платформе используется модель оплаты pay-as-you-go. С баланса каждый час списываются средства за предыдущий час использования ресурсов облачной платформы, а также оплачивается внешний трафик.

Все созданные ресурсы оплачиваются, даже если они выключены.

Например, вы создали ноды кластера Managed Kubernetes с ресурсами: vCPU, RAM и Локальный диск. Если вы выключите или приостановите ноды кластера, ресурсы продолжат оплачиваться каждый час.

Подробнее об оплате в документе Условия использования отдельных сервисов: группа услуг Облачная платформа.

Ресурсы Bare-metal Kubernetes

При создании кластера Bare-metal Kubernetes на выделенном сервере для него устанавливается тарифный план. Тарифный план определяет продолжительность оплаченного периода и сумму платежа. Платежный день устанавливается в день сдачи выделенного сервера, вместе с этим начинается первый оплаченный период.

Платежный день, сумму платежа и продолжительность оплаченного периода можно посмотреть в панели управления на странице сервера → вкладка **Услуги**.

Когда оплаченный период заканчивается, сервер автоматически продлевается на такой же период.

Например, кластер Bare-metal Kubernetes на выделенном сервере создан 10 сентября 2024 года с тарифным планом шесть месяцев и стоимостью 8 000 ₽/месяц. Размер единовременного платежа при создании кластера на выделенном сервере (с учетом скидки 7%) — 44 640 ₽. Следующий платеж для выделенного сервера будет 10 февраля 2025. Сервер автоматически будет продлен на шесть месяцев, размер платежа будет рассчитываться исходя из стоимости выделенного сервера на момент продления.

Оплата списывается единовременным платежом за весь период. При оплате сначала списываются бонусы, затем основные средства. Если бонусов недостаточно, остаток списывается из основных средств исходя из расчета суточной стоимости сервера — за сутки одним типом средств.

Например, сервер стоит 3 000 ₽/месяц, один день стоит 100 ₽. Допустим, основных средств 850 ₽, а бонусов — 2 450 ₽. Тогда при продлении услуги сначала спишутся 2 400 ₽ бонусами, а затем 600 ₽ основными средствами.

Виды тарифных планов выделенного сервера:

- 1 день;
- 1 месяц;
- 3 месяца — скидка 3%;
- 6 месяцев — скидка 7%;
- 12 месяцев — скидка 15%;
- 12 месяцев, оплата ежемесячно — скидка 10%.

Трафик

Внутренний трафик

Внутренний трафик — это входящий и исходящий трафик между объектом облачной платформы или выделенным сервером и другим продуктом Selectel, например объектным хранилищем.

Трафик между проектами и пулами облачной платформы Selectel тоже относится к внутреннему.

Внутренний трафик (входящий и исходящий) не оплачивается.

Внешний трафик

Внешний трафик — это входящий и исходящий трафик между публичным адресом объекта облачной платформы и публичным адресом в интернете. В кластерах Managed Kubernetes на облачных серверах и Bare-metal Kubernetes на выделенных серверах весь внешний трафик направляется через публичный адрес облачного роутера. Остальной трафик относится к внутреннему.

На все проекты в рамках одного аккаунта облачной платформы каждый месяц предоставляются 3 ТБ бесплатного внешнего трафика. После использования бесплатных 3 ТБ внешний трафик оплачивается по модели оплаты облачной платформы.

По умолчанию для облачной платформы включена базовая защита Selectel от DDoS-атак. Вредоносный отфильтрованный DDoS-трафик не учитывается в потреблении и не тарифицируется.

Посмотреть потребление ресурсов облачной платформы

Посмотреть текущую стоимость всей облачной инфраструктуры, потребление и оплату инфраструктуры и внешнего трафика можно в панели управления в разделе **Облачная платформа** → **Потребление платформы**.

Текущая стоимость

Текущая стоимость — это количество денег, которое потребляет текущая конфигурация облачной инфраструктуры за определенное время.

Текущую стоимость можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Текущая стоимость**.

Можно посмотреть текущую стоимость определенных проектов, ресурсов и пулов за час, день или месяц.

Данные о стоимости инфраструктуры обновляются каждый час. В панели управления они отображаются на 5–35 минут позже реального изменения инфраструктуры и ее стоимости. Недавно удаленные ресурсы могут продолжать отображаться в панели управления до следующего обновления данных. При этом ресурсы перестают тарифицироваться со следующего часа после удаления.

Графики потребления и оплаты

Графики потребления и оплаты инфраструктуры можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **График расходов** → вкладки **Потреблено** и **Оплачено**.

Можно посмотреть потребление определенных проектов, объектов, ресурсов, регионов и пулов. Графики потребления и оплаты можно посмотреть за определенный период времени или отсортировать по дням, неделям, месяцам, годам.

Чтобы выгрузить детализацию потребления и оплаты в формате `.csv`, нажмите **Скачать CSV** и выберите, как будут сгруппированы строки в выгрузке (по часам, дням, неделям, месяцам, годам).

Все блокировки ресурсов отображаются на графиках потребления и графиках оплаты.

Трафик

Потребление внешнего трафика за текущий месяц можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Внешний трафик**.

Чтобы выгрузить детализацию потребления внешнего и внутреннего трафика за каждый час по всем публичным адресам аккаунта в формате `.csv`, выберите период и нажмите **Скачать CSV**. Можно выгрузить детализацию только за последние три месяца.

Блокировка ресурсов, если на балансе недостаточно средств

Ресурсы облачной платформы

Если на момент списания на балансе будет недостаточно средств для оплаты, то все ресурсы облачной платформы автоматически заблокируются — при этом за них продолжит начисляться плата.

Чтобы восстановить доступ к ресурсам, нужно пополнить баланс на сумму долга в течение 14 дней после блокировки. Долг за ресурсы, которые тарифицировались в период блокировки, автоматически погасится. Проекты не блокируются — можно удалить проект целиком или ресурсы через API.

Если в течение 14 дней после блокировки не пополнить баланс на сумму долга, все ресурсы облачной платформы удалятся. Проекты при этом не удаляются.

Чтобы не пропускать пополнения баланса, вы можете настроить уведомления о состоянии баланса.

Ресурсы Bare-metal Kubernetes

Если на момент списания на балансе недостаточно средств для полной оплаты, сервер продлится и продолжит тарифицироваться посуточно некоторое время, в зависимости от тарифного плана:

- сервер с тарифными планами 1 месяц, 3 месяца, 6 месяцев и 12 месяцев — через четыре дня блокируются порты доступа к локальной сети и интернету, через 10 дней удаляется без возможности восстановления;

- сервер с тарифным планом 1 день — сразу блокируется доступ по сети, через 24 часа удаляется без возможности восстановления.

При расчете не учитываются праздничные и выходные дни.

Если на балансе недостаточно средств для оплаты за сутки, сервер будет тарифицироваться в долг. Долг не сгорает после удаления сервера.

Например, следующий платеж для вашего сервера с тарифным планом 6 месяцев и стоимостью 8 000 ₽/месяц — 11 октября 2024. При продлении должно быть единовременно списано 48 000 ₽. При формировании платежа стоимость сервера пересчитывается. Допустим, она повысилась до 8 100 ₽/месяц и к списанию получилось 48 600 ₽, а на вашем счете недостаточно средств. Тогда при продлении будет рассчитана и списана суточная стоимость сервера — 48 600 ₽ ÷ 182 дня = 267 ₽. Оплата будет списываться посуточно, пока на баланс не поступит сумма для полного списания (за вычетом уже оплаченных дней). Если оплата не поступит, через четыре дня для сервера будут заблокированы порты доступа к локальной сети и интернет. Через 10 дней сервер и все данные на нем будут удалены без возможности восстановления.

Если деньги идут долго или нет возможности пополнить баланс, юридические лица могут оформить отсрочку платежа до пяти дней.

Цены

Цены на ресурсы облачной платформы и выделенный сервер можно посмотреть на selectel.ru. Цены в пулах могут различаться.

Рассчитать стоимость кластера Managed Kubernetes можно в калькуляторе ресурсов.

Отчетные документы

После оплаты можно получить отчетные документы.

Создать кластер

Сравнение кластеров на выделенном сервере и на облачном сервере

	Облачный сервер	**Bare-metal Kubernetes**
Для каких задач подходит	Для задач с неравномерной нагрузкой, когда необходимо автомасштабирование групп нод	Для задач с равномерной нагрузкой и для потоковой обработки данных
Использование ресурсов	На одном хосте может быть несколько клиентов: ● если один из клиентов использует все ресурсы хоста, это влияет на производительность других клиентов этого хоста; ● из-за использования одной полосы пропускания DDoS-атаки на одного клиента могут затронуть других клиентов	Выделенные ресурсы и изолированность от других клиентов
Оплата	Pay-as-you-go — почасовая оплата только за использованные ресурсы	Тарифные планы с предоплатой за все заказанные ресурсы

Хранение данных	Постоянные тома (PV) на сетевых дисках. При возникновении ошибки на ноде сетевой диск сохранится и данные не потеряются	• локальное хранение (например, локальные диски, постоянные тома (PV) на этом же сервере); • внешнее хранение (например, Эластичное файловое хранилище, постоянные тома (PV) на другом сервере)
Автомасштабирование группы нод	✓	✗
Изменение размера группы нод	✓	✗
Изменение конфигурации нод	✓	✗
Конфигурации с GPU	✓	✗
Конфигурации с поддержкой Intel® SGX	✓	✗
Длительность развертывания	3-5 минут	До 60 минут
Приватный Kube API	✓	✓
Обновление сертификата кластера	✓	✓

Интеграция с Container Registry	✓	✓
Обновление минорной версии	✓	✗
Автообновление патч-версии	✓	✗
Автовосстановление нод	✓	✗
Метки	✓ (создание, изменение, удаление)	✓ (только создание вместе с группой нод)
Тейнты	✓ (создание, изменение, удаление)	✓ (только создание вместе с группой нод)
User data	✓	✗
Перезагрузка ноды	3-5 минут	5-10 минут
Переустановка ноды	✓	✗
Поддержка Terraform	✓	✗
Соответствие 152-ФЗ (УЗ-1)	✓	✓

Создать кластер Managed Kubernetes на облачном сервере

В одном проекте и в одном пуле можно создать не более 10 отказоустойчивых кластеров и 10 базовых кластеров Managed Kubernetes на облачных серверах.

1. Настройте кластер.
2. Настройте группу нод.
3. Настройте автоматизацию.

1. Настроить кластер
    1. В панели управления перейдите в раздел **Облачная платформа** → **Kubernetes**.

    2. Нажмите **Создать кластер**.

3. Введите имя кластера. Имя будет отображаться в именах объектов кластера: группах нод, нодах, балансировщиках, сетях и дисках. Например, если имя кластера `kelsie`, то имя группы нод будет `kelsie-node-gdc8q`, а загрузочного диска — `kelsie-node-gdc8q-volume`.

4. Выберите регион и пул, в которых будут находиться мастер-ноды. После создания кластера регион и пул нельзя изменить.

5. Выберите версию Kubernetes. После создания кластера можно обновить версию Kubernetes.

6. Выберите тип кластера:

    - отказоустойчивый — Control Plane размещен на трех мастер-нодах, которые запускаются на разных хостах в разных сегментах одного пула. Если одна из трех мастер-нод недоступна, Control Plane продолжит работать;
    - базовый — Control Plane размещен на одной мастер-ноде, которая запускается на одном хосте в одном сегменте пула. Если мастер-нода недоступна, Control Plane не будет работать.

7. После создания кластера тип кластера нельзя изменить.

8. Опционально: чтобы кластер был доступен по приватной сети и был недоступен из интернета, отметьте чекбокс **Приватный kube API**. По умолчанию кластер создается в публичной сети и ему автоматически присваивается публичный IP-адрес kube API, доступный из интернета. После создания кластера тип доступа к kube API нельзя изменить.

9. Нажмите **Продолжить**.

2. Настроить группу нод

1. В поле **Тип сервера** выберите **Облачный сервер**.

2. Выберите сегмент пула, в котором будут располагаться все рабочие ноды в группе. После создания кластера сегмент пула нельзя изменить.

3. Нажмите **Выбрать конфигурацию** и выберите конфигурацию рабочих нод в группе:

    - произвольную — можно указать любое соотношение ресурсов;
    - или фиксированную с GPU — готовые конфигурации нод с графическими процессорами и с заданным соотношением ресурсов.

    Если стандартные конфигурации не подходят, после создания кластера можно добавить группу нод с фиксированной конфигурацией облачного сервера через API Managed Kubernetes или Terraform.

3.1. Если вы выбрали произвольную конфигурацию, укажите количество vCPU, RAM, выберите загрузочный диск. Укажите размер диска.

3.2. Если вы выбрали фиксированную конфигурацию с GPU, выберите готовую конфигурацию нод с графическими процессорами, загрузочный диск и укажите размер диска. Чтобы установить драйверы GPU самостоятельно, отключите тумблер **Драйверы GPU**. По умолчанию тумблер **Драйверы GPU** включен и в кластере используются предустановленные драйверы.

3.3. Нажмите **Сохранить**.

4. Укажите количество рабочих нод в группе.

5. Опционально: чтобы сделать группу нод прерываемой, отметьте чекбокс **Прерываемая группа нод**. Прерываемые группы нод доступны только в сегментах пула ru-7a и ru-7b.

6. Опционально: чтобы включить автомасштабирование, отметьте чекбокс **Автомасштабирование группы нод**. Установите минимальное и максимальное количество нод в группе — значение нод будет меняться только в этом диапазоне. Для групп нод с GPU без драйверов автомасштабирование недоступно.

7. Опционально: чтобы добавить метки группы нод, откройте блок **Дополнительные настройки — метки, тейнты, user data**. В поле **Метки** нажмите **Добавить**. Введите ключ и значение метки. Нажмите **Добавить**.

8. Опционально: чтобы добавить тейнты группы нод, откройте блок **Дополнительные настройки — метки, тейнты, user data**. В поле **Тейнты** нажмите **Добавить**. Введите ключ и значение тейнта. Выберите эффект:

    - NoSchedule — новые поды не будут добавляться, а существующие продолжат работу;
    - PreferNoSchedule — новые поды будут добавляться, если в кластере нет других свободных мест;
    - NoExecute — запущенные поды без tolerations будут убраны.

9. Нажмите **Добавить**.

10. Опционально: чтобы добавить скрипт с пользовательскими параметрами для настройки кластера Managed Kubernetes, откройте блок **Дополнительные настройки — метки, тейнты, user data**. В поле **User Data** вставьте скрипт. Примеры скриптов и поддерживаемые форматы можно посмотреть в инструкции User data.

11. Опционально: чтобы добавить дополнительную группу рабочих нод в кластере, нажмите **Добавить группу нод**. Можно создать кластер с группами рабочих нод в разных сегментах одного пула. Это повысит отказоустойчивость и поможет

сохранить доступность приложения, если случится авария в одном из сегментов.

12. В блоке **Сеть** выберите приватную подсеть без доступа из интернета, в которую будут объединены все ноды кластера.

    Чтобы создать приватную подсеть, в поле **Подсеть для нод** выберите **Новая приватная подсеть**. Автоматически будут созданы приватная сеть `cluster_name-network`, приватная подсеть и роутер `<cluster_name>-router`, где `cluster_name` — название кластера. CIDR назначается автоматически.

    Если приватная подсеть создана, в поле **Подсеть для нод** выберите существующую подсеть. Подсеть должна соответствовать условиям:

    - подсеть должна быть подключена к облачному роутеру;
    - подсеть не должна пересекаться с диапазонами 10.250.0.0/16, 10.10.0.0/16 и 10.96.0.0/12. Эти диапазоны участвуют во внутренней адресации Managed Kubernetes;
    - в подсети должен быть выключен DHCP.
13. Нажмите **Продолжить**.

3. Настроить автоматизацию

1. Опционально: чтобы включить автовосстановление нод, отметьте чекбокс **Восстанавливать ноды**. Если у кластера всего одна рабочая нода, то автовосстановление недоступно.

2. Опционально: чтобы включить автообновление патч-версий, отметьте чекбокс **Устанавливать патч-версии**. Если у кластера всего одна рабочая нода, то автообновление патч-версий Kubernetes недоступно.

3. Выберите время начала обслуживания кластера — время, когда будут начинаться автоматические действия по обслуживанию кластера.

4. Опционально: чтобы включить аудитные логи, отметьте чекбокс **Аудитные логи**. После создания кластера настройте интеграцию с системой хранения и анализа логов.

5. Проверьте цену кластера на облачном сервере.

6. Нажмите **Создать**. Создание кластера занимает несколько минут, в это время кластер будет находиться в статусе `CREATING`. Кластер будет готов к работе, когда перейдет в статус `ACTIVE`.

Создать кластер Bare-metal Kubernetes на выделенном сервере

Вы можете создать кластер Bare-metal Kubernetes с группой нод на выделенном сервере.

Выделенные серверы используют, когда необходимы:

- стабильно высокая производительность;
- повышенный уровень конфиденциальности;
- зарезервированные мощности.

В Bare-metal Kubernetes можно использовать выделенные серверы готовой конфигурации с локальным портом.

Выделенный сервер уже собран, смонтирован и объединен в приватную сеть на уровне L3 с Kubernetes Control Plane с помощью глобального роутера.

В одном проекте и в одном пуле можно создать не более 10 отказоустойчивых кластеров и 10 базовых кластеров Bare-metal Kubernetes на выделенных серверах.

1. Настройте кластер.
2. Настройте группу нод.
3. Настройте автоматизацию.

1. Настроить кластер

1. В панели управления перейдите в раздел **Облачная платформа** → **Kubernetes**.

2. Нажмите **Создать кластер**.

3. Введите имя кластера. Имя будет отображаться в именах объектов кластера: группах нод, нодах, балансировщиках, сетях и дисках. Например, если имя кластера `kelsie`, то имя группы нод будет `kelsie-node-gdc8q`, а загрузочного диска — `kelsie-node-gdc8q-volume`.

4. Выберите регион и пул, в которых будут находиться мастер-ноды. После создания кластера пул нельзя изменить.

5. Выберите версию Kubernetes **1.28**.

6. Выберите тип кластера:

    - отказоустойчивый — Control Plane размещен на трех мастер-нодах, которые запускаются на разных хостах в разных сегментах одного пула. Если одна из трех мастер-нод недоступна, Control Plane продолжит работать;
    - базовый — Control Plane размещен на одной мастер-ноде, которая запускается на одном хосте в одном сегменте пула. Если мастер-нода недоступна, Control Plane не будет работать.

7. После создания кластера тип кластера нельзя изменить.

8. Опционально: чтобы кластер был доступен по приватной сети и был недоступен из интернета, отметьте чекбокс **Приватный kube API**. По умолчанию кластер создается в публичной сети и ему автоматически присваивается публичный IP-адрес kube API, доступный из интернета. После создания кластера тип доступа к kube API нельзя изменить.

9. Нажмите **Продолжить**.

2. Настроить группу нод

1. В поле **Тип сервера** выберите **Выделенный сервер**.

2. Выберите пул, в котором будут располагаться все рабочие ноды в группе. Рабочие ноды должны находиться в одной зоне доступности с мастер-нодами. После создания кластера пул нельзя изменить.

3. Нажмите **Выбрать конфигурацию** и выберите конфигурацию рабочих нод в группе:

   3.1. Выберите тарифный план.

   3.2. Выберите готовую конфигурацию выделенных серверов.

   3.3. Нажмите **Выбрать**.

   После создания кластера конфигурацию нод нельзя изменить.

4. Укажите количество рабочих нод в группе.

5. Опционально: чтобы добавить метки группы нод, в поле **Метки** нажмите **Добавить**. Введите ключ и значение метки. Нажмите **Добавить**. После создания кластера нельзя создать новые метки, изменить существующие метки и удалить метки.

6. Опционально: чтобы добавить тейнты группы нод, в поле **Тейнты** нажмите **Добавить**. Введите ключ и значение тейнта. Выберите эффект:

   - NoSchedule — новые поды не будут добавляться, а существующие продолжат работу;
   - PreferNoSchedule — новые поды будут добавляться, если в кластере нет других свободных мест;
   - NoExecute — запущенные поды без tolerations будут убраны.

7. Нажмите **Добавить**.

   После создания кластера нельзя создать новые тейнты, изменить существующие

тейнты и удалить тейнты.

8. Нажмите **Продолжить**.

3. Настроить автоматизацию

1. Выберите время начала обслуживания кластера — время, когда будут начинаться автоматические действия по обслуживанию кластера.

2. Опционально: чтобы включить аудитные логи, отметьте чекбокс **Аудитные логи**. После создания кластера настройте интеграцию с системой хранения и анализа логов.

3. Проверьте цену кластера на выделенном сервере.

4. Нажмите **Создать**. Создание кластера занимает до 60 минут, в это время кластер будет находиться в статусе `CREATING`. Кластер будет готов к работе, когда перейдет в статус `ACTIVE`.

   Автоматически будут созданы приватная сеть `cluster_name-network`, приватная подсеть, VLAN и глобальный роутер `<cluster_name>-router`, где `cluster_name` — название кластера. CIDR подсети выделенного сервера и CIDR подсети облачной инфраструктуры назначаются автоматически.

Работа с кластером

Подключиться к кластеру

Для начала работы с кластером нужно настроить kubectl.

Мы рекомендуем производить все действия с нодами, балансировщиками и дисками кластера только через kubectl.

После обновления сертификатов для системных компонентов необходимо заново подключаться к кластеру.

1. Установите консольный клиент Kubernetes kubectl по официальной инструкции.
2. В панели управления перейдите в раздел **Облачная платформа** → **Kubernetes**.
3. Откройте страницу кластера → вкладка **Настройки**.
4. Если вы используете приватный kube API, проверьте доступ к нему. IP-адрес указан в поле **Kube API**.
5. Нажмите **Скачать kubeconfig**.
6. Экспортируйте в переменную окружения `KUBECONFIG` путь к kubeconfig-файлу:

```
Unset
export KUBECONFIG=<path>
```

Укажите `<path>` — путь к kubeconfig-файлу `имя_кластера.yaml`.

Проверьте корректность настройки — обратитесь к кластеру через kubectl:

```
Unset

kubectl get nodes
```

Ноды должны быть в статусе `Ready`.

Логи в кластере Managed Kubernetes

В кластерах Managed Kubernetes можно получать логи — логи кластера, логи контейнеров и аудитные логи.
В логах кластера отображаются события, которые происходят с кластером. Например, создание кластера, изменение групп нод, обновление сертификатов и версии. Если запрос был выполнен автоматически, например, произошло обновление сертификатов по расписанию, то это действие тоже попадет в логи. Вы можете посмотреть логи кластера в панели управления.
В логи контейнеров попадают события, которые происходят с контейнерами. Например, создание и удаление контейнера. Файлы логов контейнеров хранятся в каталоге `/var/log/pods/` или `/var/log/containers`. Логи отдельного контейнера можно посмотреть с помощью `kubectl logs <container_name>`, где `<container_name>` — имя контейнера. Если в кластере Managed Kubernetes много контейнеров, вы можете настроить получение логов контейнеров через Filebeat.
В аудитных логах отображаются события, которые происходят в кластере. Например, в подах или сервисах. Эти события могут быть инициированы пользователями, приложениями или Control Plane. Список событий, которые попадают в логи, и параметры этих событий зависят от политики (audit policy). Политику, которая применяется для аудитных логов Managed Kubernetes, можно посмотреть в документации Selectel на сайте GitHub.
Аудитные логи можно хранить в системе хранения и анализа логов. Например, во внешних хранилищах данных (например, Elasticsearch или Stackdriver) или в SIEM-системе (например, MaxPatrol SIEM или KUMA). Чтобы получать аудитные логи из кластера Managed Kubernetes в системе хранения и анализа логов, настройте интеграцию.

Посмотреть логи кластера

1. В панели управления перейдите в раздел **Облачная платформа** → **Kubernetes**.
2. Откройте страницу кластера → вкладка **Логи**.
3. Посмотрите статус событий кластера в строке события → столбец **Статус**.

IN_PROGRESS	Событие выполняется
IN_QUEUE	Событие в очереди. Ожидается завершение события со статусом `IN_PROGRESS`
CANCELED	Событие отменено
ERROR	Произошла ошибка. Если причина ошибки — нехватка квот в проекте, увеличьте квоты. Если причина не указана, создайте тикет

DONE	Событие успешно завершилось

Настроить получение логов контейнеров через Filebeat

Filebeat по умолчанию настроен на работу с Docker. В Selectel вместо Docker в качестве среды исполнения контейнеров (CRI) используется containerd.
Чтобы настроить механизм получения метаданных логов через Filebeat, используйте конфигурационный файл:

```
Unset
filebeat.inputs:
- type: container
  fields_under_root: true
  paths:
  - "/var/log/containers/*.log"
  processors:
    - add_kubernetes_metadata:
        host: ${NODE_NAME}
        in_cluster: true
        default_matchers.enabled: false
        matchers:
        - logs_path:
            logs_path: "/var/log/containers/"
```

Настроить интеграцию с системой хранения и анализа логов

Аудитные логи доступны, если вы используете версию Kubernetes 1.28 и выше. В кластерах Managed Kubenretes на облачных серверах вы можете обновить версию кластера. Во время обновления версии аудитные логи недоступны.
Система хранения и анализа логов, которую вы используете, должна быть доступна по протоколу HTTPS.

1. Включите аудитные логи — при создании кластера или в существующем кластере.
2. Подключитесь к кластеру.
3. Настройте экспорт аудитных логов в систему хранения и анализа логов.

1. Включить аудитные логи в существующем кластере

1. В панели управления перейдите в раздел **Облачная платформа** → **Kubernetes**.
2. Откройте страницу кластера → вкладка **Настройки**.
3. В блоке **Логирование** включите тумблер **Аудитные логи**.

2. Подключиться к кластеру

Используйте инструкцию Подключиться к кластеру для нужной операционной системы.

3. Настроить экспорт аудитных логов в систему хранения и анализа логов

Аудитные логи начнут передаваться в систему хранения и анализа логов после создания объекта Secret.

1. Создайте yaml-файл с манифестом для объекта Secret:

```
Unset
apiVersion: v1
kind: Secret
metadata:
  name: mks-audit-logs
data:
  host: <host>
  port: <port>
  username: <username>
  password: <password>
  ca.crt: <ca_certificate>
```

Укажите:

- `<host>` — DNS- или IP-адрес системы хранения и анализа логов;
- `<port>` — порт для подключения к системе хранения и анализа логов;
- опционально: `<username>` — имя пользователя системы хранения и анализа логов;
- опционально: `<password>` — пароль пользователя системы хранения и анализа логов;
- опционально: `<ca_certificate>` — сертификат из приватного центра сертификации (CA). Если для подключения используется Let's Encrypt сертификат, этот параметр не нужно заполнять.

2. Примените манифест и создайте объект Secret в пространстве имен `kube-system`:

```
Unset
kubectl apply -f <secret.yaml> --namespace=kube-system
```

Укажите `<secret.yaml>` — имя yaml-файла с манифестом для создания нового объекта Secret.

3. Проверьте, что объект Secret создан:

```
Unset
kubectl get secret mks-audit-logs --output=yaml
--namespace=kube-system
```

Развернуть образ из Container Registry

Если вы храните Docker-образы в Container Registry, вы можете развернуть под в кластере Managed Kubernetes.

1. Загрузите образ в реестр Container Registry.
2. Настройте интеграцию Container Registry с кластером.
3. Разверните приложение из образа.

Feature Gates

С Feature Gates доступны дополнительные возможности для компонента kube-apiserver.

Каждое дополнение имеет определенную стадию (stage) в зависимости от версии Kubernetes:

- Alpha — отключены по умолчанию, можно включить.
- Beta — включены по умолчанию только до версии Kubernetes 1.24, подробнее в статье Feature Gates документации Kubernetes. Нельзя отключить из-за политики поддержания стабильности работы кластера.
- GA (General Availability) — внесены в ядро kube-apiserver, включены по умолчанию, нельзя отключить.

Для активации Feature Gates необходимо при создании или обновлении кластера указать в виде списка названия необходимых дополнений. Далее kube-apiserver будет запущен или перезапущен с опцией `--feature-gates=...` и заданными дополнениями.

При передаче дополнения, использование которого недоступно для текущей версии Kubernetes, будет возвращена соответствующая ошибка.

Получить информацию о доступных контроллерах для каждой из доступных версий Kubernetes можно с помощью запроса к API Managed Kubernetes.

Admission Controllers

Admission Controllers (контроллеры доступа) позволяют добавить дополнительные опции в работу Kubernetes для изменения или валидации объектов при запросах к Kubernetes

API. Если в результате работы контроллера запрос отклоняется, то отклоняется весь запрос к API-серверу, а конечному пользователю возвращается ошибка.

Чтобы активировать контроллеры доступа, необходимо при создании или обновлении кластера указать названия контроллеров в виде списка. После этого kube-apiserver будет запущен или перезапущен с опцией `--enable-admission-plugins` и заданными контроллерами доступа.

При передаче контроллера, использование которого недоступно для текущей версии Kubernetes, будет возвращена соответствующая ошибка.

Получить информацию о доступных контроллерах для каждой из доступных версий Kubernetes можно с помощью запроса к API Managed Kubernetes.

Metrics Server

Metrics Server — это компонент Kubernetes, который собирает данные об использовании ресурсов в кластере и через Metrics API передает их в другие компоненты Kubernetes. На основании данных от Metrics Server работает горизонтальное (Horizontal Pod Autoscaling) и вертикальное автомасштабирование подов (Vertical Pod Autoscaling). Посмотреть метрики можно с помощью `kubectl top`. Автомасштабирование групп нод на облачных серверах можно настроить с помощью Cluster Autoscaler. Для мониторинга смотрите логи в кластере Managed Kubernetes или используйте специальные приложения, например Prometheus.

Metrics Server установлен по умолчанию в кластерах Managed Kubernetes версии 1.27 и выше. Вы можете обновить версию кластера на облачном сервере.

Подробнее о работе Metrics Server в статье Kubernetes Metrics Server в документации Kubernetes.

Удалить кластер Managed Kubernetes

При удалении кластера удаляются все его компоненты: ноды, диски и балансировщики нагрузки.

1. В панели управления перейдите в раздел **Облачная платформа → Kubernetes**.
2. Откройте страницу кластера.
3. В меню ⋮ кластера выберите **Удалить**.

Работа с группами нод

Конфигурации нод Managed Kubernetes

В кластере Managed Kubernetes для создания групп нод можно использовать конфигурации на облачном сервере и конфигурации на выделенном сервере.

Посмотреть доступность конфигураций в регионах можно в матрице доступности Managed Kubernetes.

Конфигурации нод на облачном сервере

Для нод на облачном сервере доступно три типа конфигураций:

- произвольные конфигурации — можно указать любое соотношение ресурсов;
- фиксированные конфигурации с GPU — готовые конфигурации нод с графическими процессорами и с заданным соотношением ресурсов;
- другие фиксированные конфигурации (флейворы) облачных серверов — несколько линеек с разными техническими характеристиками, в которых зафиксировано соотношение ресурсов. Можно добавить только через API Managed Kubernetes или Terraform.

Сравнить доступные конфигурации можно в таблице Сравнение конфигураций нод на облачном сервере.

Если вам не подходят доступные конфигурации, например, нужно больше vCPU или RAM, создайте тикет — мы подберем конфигурации с другим количеством ресурсов.

Произвольные конфигурации

В произвольных конфигурациях нод можно указать необходимое количество ресурсов. Лимиты зависят от пула, их можно посмотреть в таблице Сравнение конфигураций нод на облачном сервере.

В качестве загрузочного диска для нод можно выбрать локальный диск или один из четырех типов сетевых дисков.

Фиксированные конфигурации с GPU

Можно выбрать фиксированную конфигурацию с выделенными GPU и заданным соотношением ресурсов. Подробные характеристики графических процессоров можно посмотреть в инструкции Создать кластер Managed Kubernetes с GPU.

Конфигурации соответствуют линейке GPU Line облачных серверов.

В качестве загрузочного диска для нод можно выбрать один из четырех типов сетевых дисков.

Сравнение конфигураций нод на облачном сервере

Если стандартные конфигурации Managed Kubernetes не подходят, можно использовать фиксированные конфигурации облачных серверов.

	Произвольные конфигурации (кроме ru-3, ru-9, ru-7, ru-8)	Произвольные конфигурации (ru-3, ru-9, ru-7, ru-8)	Фиксированные конфигурации с GPU
Количество vCPU	1—8	1—32	4—48 1—8 GPU
RAM	1—64 ГБ*	4—256 ГБ*	24—700 ГБ
Размер локального диска	20—512 ГБ**	20 ГБ — 1,2 ТБ**	✗
Размер сетевого диска	20—512 ГБ	20 ГБ — 1,2 ТБ	30—512 ГБ

*Если в конфигурации больше 8 vCPU, то можно выбрать RAM с соотношением не меньше чем 1:2. Например, если вы выбрали 10 vCPU, то RAM должна быть не менее 20 ГБ.

**Если в конфигурации больше 8 vCPU, то можно выбрать размер локального диска с соотношением не меньше чем 1:32. Например, для 10 vCPU размер диска — минимум 320 ГБ.

Посмотреть доступность конфигураций можно в матрице доступности Managed Kubernetes и GPU для облачных серверов и Managed Kubernetes.

Конфигурации нод Bare-metal Kubernetes

В кластерах Bare-metal Kubernetes можно создать ноды на выделенных серверах готовых конфигураций, которые соответствуют требованиям:

- есть локальный порт;
- процессор x86;
- сетевая карта 1 Гбит/с;
- без поддержки Intel® SGX;
- без GPU.

Посмотреть подробную информацию о конфигурациях можно в конфигураторе.

Выделенные серверы собираются и монтируются в стойки заранее, готовы к работе в течение одного часа после создания кластера или группы нод (без учета времени на установку ОС).

Прерываемые группы нод

В прерываемой группе нод каждая из нод работает не более 24 часов. В это время ноды могут быть остановлены со стороны Selectel в любой момент — например, если на виртуальном хосте не хватает ресурсов для других кластеров.

Восстановление запустится сразу после остановки. Если свободных ресурсов достаточно для восстановления, то длительность восстановления ноды будет зависеть от типа загрузочного диска:

- нода с сетевым загрузочным диском восстанавливается меньше одной минуты;
- нода с локальным загрузочным диском восстанавливается до 10 минут.

От типа загрузочного диска также зависит восстановление данных на ноде. Если используется сетевой загрузочный диск, все данные сохраняются, если локальный — удаляются.

После каждого восстановления отсчет 24 часов начинается заново.

Прерываемые группы нод поддерживают все функции, которые доступны для обычных групп нод, при этом стоимость ресурсов в таких группах ниже в среднем на 70%.

Можно сделать группу нод прерываемой в панели управления при создании кластера или добавлении группы нод. Прерываемой можно сделать группу нод любой конфигурации.

Ограничения

Прерываемые группы нод доступны только в кластерах на облачных серверах в сегментах пула ru-7a и ru-7b.

Мы не гарантируем уровень доступности как у обычных групп нод — на прерываемые группы нод не действует SLA кластера Kubernetes.

Стоимость

Стоимость ресурсов в прерываемой группе нод ниже в среднем на 70%, чем стоимость ресурсов в обычной группе нод с такой же конфигурацией.

Во время работы ресурсы в прерываемой группе нод оплачиваются по модели оплаты ресурсов облачной платформы.

После прерывания:

- за vCPU, RAM, GPU, локальные диски средства перестают списываться, начиная со следующего часа после остановки;

- за сетевые диски средства продолжают списываться.

User data

Использование user data недоступно в кластерах Bare-metal Kubernetes на выделенных серверах.

User data в кластере Managed Kubernetes на облачном сервере — пользовательские параметры для настройки и персонализации кластера. Передаются как скрипт в формате cloud-config (текстовые файлы с YAML-синтаксисом) или как bash-скрипт. Скрипты автоматически кодируются в Base64, а затем передаются на облачный сервер, на котором расположен кластер Managed Kubernetes. На сервере скрипты выполняются с помощью агента cloud-init. Использование user data помогает ускорить и автоматизировать процесс настройки кластера Managed Kubernetes.

Указать user data можно при создании кластера или добавлении новой группы нод.

Подробнее о форматах скриптов cloud-config и bash в инструкции User data formats документации cloud-init.

В скриптах можно передавать параметры для настройки рабочих нод и установки дополнительного программного обеспечения на ноды вне кластера Managed Kubernetes. Например:

- отключить IPv6;
- создать каталог и загрузить в него файлы по сети.

Указать user data

Указать user data можно при создании кластера на облачном сервере или добавлении новой группы нод:

- в панели управления — скрипт с данными, которые не закодированы в Base64, в поле **User Data**. Максимальный размер скрипта — 47 КБ;
- через Terraform — только скрипт с данными, которые закодированы в Base64, в аргумент **user_data**. Максимальный размер скрипта — 65 535 байт.

После добавления user data изменить скрипт нельзя.

Удалить группу нод

Удаленные ноды перестанут отображаться в панели управления:

- ноды на облачном сервере — в разделе **Облачная платформа** → **Серверы**;
- ноды Bare-metal Kubernetes на выделенном сервере — в разделе **Серверы и оборудование** → **Серверы**.

1. В панели управления перейдите в раздел **Облачная платформа** → **Kubernetes**.
2. Откройте страницу кластера → вкладка **Состав кластера**.
3. В меню группы нод ⋮ выберите **Удалить группу**.

Работа с дисками

Диски Managed Kubernetes

Managed Kubernetes использует локальные и сетевые диски облачной платформы.

Локальные и сетевые диски в кластере Managed Kubernetes вы можете использовать в качестве загрузочного диска и для хранения данных.

При выборе диска учтите особенности использования локальных и сетевых дисков в Kubernetes.

Использование сетевых и локальных дисков в Kubernetes

	Локальные диски	**Сетевые диски**
Преимущества	Низкая задержка доступа к данным	Возможность хранения постоянных данных, которые нужно сохранять при перезапуске и миграции подов
Ограничения	Нет доступности данных между подами	Есть дополнительная сетевая задержка доступа к данным
Объекты в Kubernetes	Volume и VolumeMounts, PersistentVolumes и PersistentVolumeClaims (при самостоятельной установке CSI-драйвера)	PersistentVolumes и PersistentVolumeClaims
Использование	• Загрузочный диск • Хранение данных	• Загрузочный диск • Хранение данных

Загрузочные диски

Загрузочные (системные) диски используются для запуска и инициализации операционной системы и приложений в контейнерах Kubernetes.

В качестве загрузочных дисков можно использовать локальные и сетевые диски облачной платформы.

Загрузочный диск вы выбираете при создании кластера и не можете изменить его после создания кластера.

При переустановке нод все данные на загрузочных дисках удаляются.

Ноды переустанавливаются:

- при обновлении минорной версии кластера;
- переустановке нод вручную;
- автообновлении патч-версий;
- автовосстановлении нод.

Диски для хранения данных

Для хранения данных в кластерах Managed Kubernetes рекомендуем использовать PersistentVolume (PV) на сетевых дисках.

Если вы самостоятельно установили CSI-драйвер и создали PV на локальном диске, то при удалении ноды данные будут удалены.

Работа с сетью

Терминировать TLS-соединения

Терминирование TLS-соединения для кластера Managed Kubernetes — это процесс расшифровки HTTPS-трафика и перенаправления его на поды Kubernetes в виде HTTP-трафика.

Терминирование TLS-соединения может использоваться:

- для защиты передачи данных между клиентом и сервисом в кластере;
- контроля доступа к сервисам в кластере и защиты от несанкционированного доступа;
- повышения производительности;
- упрощения управления сертификатами.

В кластере Managed Kubernetes процесс терминирования TLS-соединений можно настроить на балансировщике нагрузки.

Сертификатами можно управлять через менеджер секретов — добавьте свой пользовательский сертификат или выпустите сертификат Let's Encrypt®.

Терминирование TLS-соединения на балансировщике нагрузки доступно, если вы используете версии Kubernetes 1.25 и выше. Вы можете обновить версию кластера.

1. Добавьте пользовательский сертификат или выпустите его в менеджере секретов.
2. Создайте балансировщик нагрузки.
3. Измените A-запись домена.

Container Registry

Общая информация

Container Registry as a Service (CRaaS) — это полностью готовый к работе реестр контейнеров для хранения и развертывания Docker-образов.

Вы можете создать приватный реестр и управлять образами через Docker CLI — загружать, скачивать и удалять их. Образы в реестре хранятся с тройной репликацией.

Если вы используете Container Registry, образы и инфраструктура находятся у одного провайдера — это ускоряет развертывание, загрузку и скачивание образов.

В Container Registry вы также можете хранить Helm-чарты и управлять ими через Helm CLI.

Работать с Container Registry можно в панели управления, через API Container Registry или с помощью Terraform.

В продукте поддерживаются типы и роли пользователей, проекты и лимиты проекта и квоты.

Реестр и репозиторий

Container Registry — это реестр для хранения Docker-образов и Helm-чартов.

В одном репозитории можно хранить несколько версий одного образа или чарта с одинаковым именем.

В одном реестре можно создать несколько репозиториев.

Тег и хеш

Версии образов можно различать с помощью тегов или хешей. Хеш генерируется автоматически и является уникальным, а тег нужно назначить самостоятельно.

Если при загрузке образа не указать тег, то автоматически установится тег `latest`.

Если загрузить версию образа с тегом, который уже используется в репозитории, то тег добавится к новой версии и удалится у старой.

Тег для обращения к образу выглядит так:

```
Unset
cr.selcloud.ru/<registry>/<image>:<tag>
```

Токен

Токен необходим для авторизации в Container Registry и получения доступа к реестру.

Токенами можно управлять через API Container Registry или в панели управления.

Ограничения

В одном проекте можно создать не более 100 реестров.

Модель оплаты и цены Container Registry

Баланс

Для оплаты ресурсов облачной платформы в зависимости от типа баланса в аккаунте используется единый баланс или баланс облачной платформы.

Оплатить ресурсы можно разными типами средств: основными средствами, бонусами или ВК бонусами.

Перед оплатой пополните баланс.

Модель оплаты

В облачной платформе используется модель оплаты pay-as-you-go. С баланса каждый час списываются средства за предыдущий час использования ресурсов облачной платформы. В Container Registry оплачивается хранение образов и чартов и исходящий внешний трафик.

Подробнее об оплате в документе Условия использования отдельных сервисов: группа услуг Облачная платформа.

Блокировка ресурсов, если на балансе недостаточно средств

Если на момент списания на балансе будет недостаточно средств для оплаты, то все ресурсы облачной платформы автоматически заблокируются — при этом за них продолжит начисляться плата.

Чтобы восстановить доступ к ресурсам, нужно пополнить баланс на сумму долга в течение 14 дней после блокировки. Долг за ресурсы, которые тарифицировались в период блокировки, автоматически погасится. Проекты не блокируются — можно удалить проект целиком или ресурсы через API.

Если в течение 14 дней после блокировки не пополнить баланс на сумму долга, все ресурсы облачной платформы удалятся. Проекты при этом не удаляются.

Чтобы не пропускать пополнения баланса, вы можете настроить уведомления о состоянии баланса.

Внешний трафик

Внешний трафик — это входящий и исходящий трафик между Container Registry и публичными адресами в интернете. Остальной трафик относится к внутреннему.

Входящий внешний трафик до Container Registry бесплатный.

Исходящий внешний трафик от Container Registry оплачивается по модели оплаты облачной платформы после использования бесплатных 10 ГБ.

Внутренний трафик

Внутренний трафик — это входящий и исходящий трафик между Container Registry и другими услугами Selectel, например Managed Kubernetes.

Трафик между проектами и пулами облачной платформы Selectel тоже относится к внутреннему.

Со стороны облачной платформы трафик (входящий и исходящий) до любых других услуг Selectel не оплачивается.

Посмотреть потребление

Посмотреть текущую стоимость всей облачной инфраструктуры, потребление и оплату инфраструктуры и внешнего трафика можно в панели управления в разделе **Облачная платформа** → **Потребление платформы**.

Текущая стоимость

Текущая стоимость — это количество денег, которое потребляет текущая конфигурация облачной инфраструктуры за определенное время.

Текущую стоимость можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Текущая стоимость**.

Можно посмотреть текущую стоимость определенных проектов, ресурсов и пулов за час, день или месяц.

Данные о стоимости инфраструктуры обновляются каждый час. В панели управления они отображаются на 5–35 минут позже реального изменения инфраструктуры и ее стоимости. Недавно удаленные ресурсы могут продолжать отображаться в панели управления до следующего обновления данных. При этом ресурсы перестают тарифицироваться со следующего часа после удаления.

Графики потребления и оплаты

Графики потребления и оплаты инфраструктуры можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **График расходов** → вкладки **Потреблено** и **Оплачено**.

Можно посмотреть потребление определенных проектов, объектов, ресурсов, регионов и пулов. Графики потребления и оплаты можно посмотреть за определенный период времени или отсортировать по дням, неделям, месяцам, годам.

Чтобы выгрузить детализацию потребления и оплаты в формате `.csv`, нажмите **Скачать CSV** и выберите, как будут сгруппированы строки в выгрузке (по часам, дням, неделям, месяцам, годам).

Все блокировки ресурсов отображаются на графиках потребления и графиках оплаты.

Трафик

Потребление внешнего трафика за текущий месяц можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Внешний трафик**.

Чтобы выгрузить детализацию потребления внешнего и внутреннего трафика за каждый час по всем публичным адресам аккаунта в формате `.csv`, выберите период и нажмите **Скачать CSV**. Можно выгрузить детализацию только за последние три месяца.

Цены

Цены на ресурсы и исходящий внешний трафик можно посмотреть на selectel.ru. Цены в пулах могут различаться.

Рассчитать стоимость Container Registry можно в калькуляторе ресурсов.

Отчетные документы

После оплаты можно получить отчетные документы.

Работа с реестром

Создать реестр

1. В панели управления перейдите в раздел **Облачная платформа → Container Registry**.
2. Нажмите **Начать работу**.
3. Введите имя реестра. Максимальная длина имени реестра — 20 символов UTF-8. Имя реестра будет частью его URI:

```
Unset
cr.selcloud.ru/<registry>
```

4. Нажмите **Создать**.

Удалить репозиторий

1. В панели управления перейдите в раздел **Облачная платформа → Container Registry**.
2. В строке с репозиторием нажмите 🗑️.

Удалить реестр

1. В панели управления перейдите в раздел **Облачная платформа → Container Registry**.
2. В меню ⋮ реестра выберите **Удалить реестр**.

Работа с токенами

Сгенерировать токен

Чтобы настроить доступ к реестрам, сгенерируйте токен. Вы можете выбрать срок действия токена, права доступа и реестры, к которым дает доступ токен.

1. В панели управления перейдите в раздел **Облачная платформа → Container Registry**.

2. Откройте страницу реестра.

3. Нажмите **Доступ к реестру**.

4. Нажмите **Генерация токена**.

5. Введите имя токена.

6. Выберите права доступа:

    - только на чтение — будет доступно скачивание образов и чартов из реестра;
    - на запись и чтение — будет доступно добавление, скачивание и удаление образов и чартов из реестра.
7. Выберите реестр, к которому хотите предоставить доступ. Если вы предоставляете доступ ко всем реестрам, то токен будет действителен и для новых реестров, которые вы будете создавать в этом проекте.

8. Выберите срок действия токена:

    - 30 дней;
    - 60 дней;
    - 90 дней;
    - 1 год;
    - бессрочный.
9. Нажмите **Сгенерировать токен**.

10. Когда будут созданы логин и пароль, нажмите **Скачать json-токен**.

Редактировать токен

После выпуска токена можно изменить его название, срок действия, права доступа и реестры, к которым дает доступ этот токен.

1. В панели управления перейдите в раздел **Облачная платформа** → **Container Registry**.
2. Откройте вкладку **Токены**.
3. Откройте страницу токена.
4. Внесите необходимые изменения.
5. Нажмите **Сохранить**.

Удалить токен

1. В панели управления перейдите в раздел **Облачная платформа** → **Container Registry**.
2. В меню ⋮ реестра выберите **Удалить**.
3. Чтобы подтвердить удаление токена, введите его имя.
4. Нажмите **Удалить**.

Облачные базы данных

Общая информация

Облачные базы данных — сервис для развертывания и управления высокопроизводительными и отказоустойчивыми кластерами поддерживаемых баз данных в облаке.

С облачными базами данных можно работать в панели управления, через API Облачных баз данных или Terraform.

В продукте поддерживаются типы и роли пользователей, проекты и лимиты проекта и квоты.

Поддерживаемые облачные базы данных

PostgreSQL	База данных с открытым исходным кодом. Ориентирована на скорость работы и расширяемость — можно подключать любые внешние источники данных, создавать новые типы данных и функции
PostgreSQL для 1С	Версия PostgreSQL с необходимыми расширениями для эффективной работы с 1С:Предприятие
PostgreSQL TimescaleDB	Версия PostgreSQL с расширением TimescaleDB, которую можно использовать для хранения временных рядов
MySQL semi-sync	Система управления реляционными базами данных с открытым исходным кодом, легко управляется и масштабируется. Подходит для выполнения большинства задач по работе с данными
MySQL sync	Решение для MySQL с открытым исходным кодом. Работает на базе Percona Server для MySQL с подсистемой хранения XtraDB
Redis	Система управления in-memory базами данных класса NoSQL. Может работать как база данных и система очередей
Kafka	Распределенная система с открытым исходным кодом для доставки, хранения и обработки сообщений. Может работать как шина данных для Cloud Native приложений

Как работают облачные базы данных

Облачные базы данных разворачиваются в кластере. Кластер — это один или несколько серверов баз данных (нод), между которыми настроена репликация. Ноды кластера работают на базе ресурсов облачной платформы.

Облачные базы данных поддерживают мониторинг, резервное копирование и масштабирование кластера. Можно повысить отказоустойчивость кластера и настроить репликацию между нодами.

Настройки баз данных при создании кластера подобраны по умолчанию и зависят от конфигурации кластера и версии базы данных. При необходимости вы можете их изменить.

Настройка сетей облачной базы данных зависит от особенностей инфраструктуры, в которую встраивается облачная база данных.

Мониторинг

В облачных базах данных можно отслеживать состояние кластера в панели управления:

- смотреть информацию об использовании нод кластера и о нагрузке на базы данных в виде графиков в панели управления;
- смотреть статус кластера;
- получать уведомления о заполненности диска.

Метрики нод кластера и баз данных можно также экспортировать в формате Prometheus.

Подробнее о мониторинге в инструкциях для PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync, Redis и Kafka.

Резервное копирование

В облачных базах данных резервные копии кластера создаются автоматически с помощью WAL-G. Все базы данных, кроме Redis, восстанавливаются на момент времени (Point-in-Time Recovery). Частота создания резервных копий зависит от выбранной базы данных.

Резервные копии хранятся в объектном хранилище Selectel изолированно от резервных копий других пользователей. Резервные копии нельзя выгрузить. Автоматическое создание резервных копий нельзя отключить.

Подробнее о резервном копировании в инструкциях для PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync, Redis.

Масштабирование

Кластер облачных баз данных можно масштабировать — например, увеличить vCPU и RAM для повышения производительности кластера. Также можно изменить фиксированную конфигурацию нод на произвольную конфигурацию или произвольную

конфигурацию на фиксированную, но только с бóльшим объемом дискового пространства.

Процесс изменения конфигурации зависит от наличия реплик. Время изменения конфигурации зависит от объема данных в кластере.

Подробнее о масштабировании в инструкциях для PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync, Redis и Kafka.

Отказоустойчивость и репликация

По умолчанию кластер состоит из одной главной ноды — мастер-ноды. При подключении к мастер-ноде доступны все операции: чтение (SELECT) и запись (INSERT, UPDATE, DELETE и другие). Чтобы обеспечить отказоустойчивость кластера, добавьте реплики — полные копии мастер-ноды. Они доступны только для чтения данных (SELECT). Если мастер-нода недоступна, реплики возьмут на себя ее роль, и кластер будет работать в штатном режиме. Их можно также использовать для снижения нагрузки на мастер-ноду при активном чтении.

Подробнее об отказоустойчивости в инструкциях для PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync, Redis.

Настройки облачных баз данных

Настройки базы данных влияют на производительность кластера баз данных. При создании кластера баз данных значения для всех настроек задаются автоматически. Значения подобраны так, чтобы обеспечить высокую производительность кластера, они отличаются в зависимости от конфигурации кластера и версии базы данных.

Если автоматические значения не подходят для ваших задач, для всех облачных баз данных, кроме Redis, вы можете установить свои значения при создании кластера или изменить настройки в уже созданном кластере.

Подробнее о настройках облачных баз данных в инструкциях для PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync и Kafka.

Сети

При создании кластера облачных баз данных необходимо учесть особенности инфраструктуры, в которую встраивается облачная база данных — нужен ли доступ к нодам кластера из интернета и нужна ли сетевая связность с другими услугами Selectel.

Кластер может быть подключен:

- к приватной подсети — подсеть без доступа из интернета;
- публичной подсети — все адреса публичной подсети доступны из интернета.

После создания кластера подсеть нельзя изменить.

Подробнее о создании сетевой связности между выделенным сервером Selectel и кластером облачных баз данных в инструкциях для PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync, Redis и Kafka.

Зоны ответственности

Selectel обеспечивает

- подбор оборудования для высокой производительности СУБД;
- установку операционной системы;
- установку и оптимальную настройку СУБД;
- обновление и обслуживание операционной системы и служебного ПО;
- надежность и отказоустойчивость кластера — когда вы создаете отказоустойчивый кластер, мы обеспечиваем аварийное переключение при сбое;
- настройку и обслуживание служебной сети для реплик кластера;
- резервное копирование — автоматическое создание и хранение копий;
- систему мониторинга состояния кластера в панели управления;
- безопасное хранение данных и защиту от краж и утечек;
- соответствие требованиям 152-ФЗ;
- наличие ресурсов для масштабирования кластера, если вы инициировали масштабирование;
- техническую поддержку.

Пользователь обеспечивает

- корректное подключение к базе данных;
- оптимальность написания запросов к базе данных;
- схему и структуру данных в базе;
- инициирование масштабирования кластера.

Если вам нужна помощь с администрированием баз данных, закажите услуги администрирования сервисов.

Модель оплаты и цены облачных баз данных

Баланс

Для оплаты ресурсов облачной платформы в зависимости от типа баланса в аккаунте используется единый баланс или баланс облачной платформы.

Оплатить ресурсы можно разными типами средств: основными средствами, бонусами или ВК бонусами.

Перед оплатой пополните баланс.

Модель оплаты

В облачной платформе используется модель оплаты pay-as-you-go. С баланса каждый час списываются средства за предыдущий час использования ресурсов облачной платформы, а также оплачивается внешний трафик.

Все созданные ресурсы оплачиваются, даже если они выключены.

Например, вы создали кластер облачных баз данных с ресурсами: vCPU, RAM и Локальный диск. Если кластер приостановит работу, ресурсы продолжат оплачиваться каждый час.

Подробнее об оплате в документе Условия использования отдельных сервисов: группа услуг Облачная платформа.

Блокировка ресурсов, если на балансе недостаточно средств

Если на момент списания на балансе будет недостаточно средств для оплаты, то все ресурсы облачной платформы автоматически заблокируются — при этом за них продолжит начисляться плата.

Чтобы восстановить доступ к ресурсам, нужно пополнить баланс на сумму долга в течение 14 дней после блокировки. Долг за ресурсы, которые тарифицировались в период блокировки, автоматически погасится. Проекты не блокируются — можно удалить проект целиком или ресурсы через API.

Если в течение 14 дней после блокировки не пополнить баланс на сумму долга, все ресурсы облачной платформы удалятся. Проекты при этом не удаляются.

Чтобы не пропускать пополнения баланса, вы можете настроить уведомления о состоянии баланса.

Внешний трафик

Внешний трафик — это входящий и исходящий трафик между публичным адресом объекта облачной платформы и публичным адресом в интернете. Остальной трафик относится к внутреннему.

На все проекты в рамках одного аккаунта облачной платформы каждый месяц предоставляются 3 ТБ бесплатного внешнего трафика. После использования бесплатных 3 ТБ внешний трафик оплачивается по модели оплаты облачной платформы.

По умолчанию для облачной платформы включена базовая защита Selectel от DDoS-атак. Вредоносный отфильтрованный DDoS-трафик не учитывается в потреблении и не тарифицируется.

Внутренний трафик

Внутренний трафик — это входящий и исходящий трафик между публичным адресом объекта облачной платформы и публичным адресом другой услуги Selectel, например Выделенный сервер или Объектное хранилище.

Трафик между проектами и пулами облачной платформы Selectel тоже относится к внутреннему.

Со стороны облачной платформы трафик (входящий и исходящий) до любых других услуг Selectel не оплачивается.

Посмотреть потребление

Посмотреть текущую стоимость всей облачной инфраструктуры, потребление и оплату инфраструктуры и внешнего трафика можно в панели управления в разделе **Облачная платформа** → **Потребление платформы**.

Текущая стоимость

Текущая стоимость — это количество денег, которое потребляет текущая конфигурация облачной инфраструктуры за определенное время.

Текущую стоимость можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Текущая стоимость**.

Можно посмотреть текущую стоимость определенных проектов, ресурсов и пулов за час, день или месяц.

Данные о стоимости инфраструктуры обновляются каждый час. В панели управления они отображаются на 5–35 минут позже реального изменения инфраструктуры и ее стоимости. Недавно удаленные ресурсы могут продолжать отображаться в панели управления до следующего обновления данных. При этом ресурсы перестают тарифицироваться со следующего часа после удаления.

Графики потребления и оплаты

Графики потребления и оплаты инфраструктуры можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **График расходов** → вкладки **Потреблено** и **Оплачено**.

Можно посмотреть потребление определенных проектов, объектов, ресурсов, регионов и пулов. Графики потребления и оплаты можно посмотреть за определенный период времени или отсортировать по дням, неделям, месяцам, годам.

Чтобы выгрузить детализацию потребления и оплаты в формате `.csv`, нажмите **Скачать CSV** и выберите, как будут сгруппированы строки в выгрузке (по часам, дням, неделям, месяцам, годам).

Все блокировки ресурсов отображаются на графиках потребления и графиках оплаты.

Трафик

Потребление внешнего трафика за текущий месяц можно посмотреть в панели управления в разделе **Облачная платформа** → **Потребление платформы** → вкладка **Внешний трафик**.

Чтобы выгрузить детализацию потребления внешнего и внутреннего трафика за каждый час по всем публичным адресам аккаунта в формате `.csv`, выберите период и нажмите **Скачать CSV**. Можно выгрузить детализацию только за последние три месяца.

Цены

Цены на ресурсы и внешний трафик можно посмотреть на selectel.ru. Цены в пулах могут различаться.

Рассчитать стоимость кластера облачных баз данных можно в калькуляторе ресурсов.

Отчетные документы

После оплаты можно получить отчетные документы.

PostgreSQL

Версии и конфигурации PostgreSQL

Версии

Поддерживаются версии PostgreSQL 12, 13, 14, 15 и 16.

Конфигурации нод

При создании кластера облачных баз данных PostgreSQL можно выбрать для нод количество vCPU, RAM и размер локального диска.

Доступно два типа конфигураций:

- фиксированные конфигурации — несколько линеек с разными техническими характеристиками, в которых зафиксировано соотношение ресурсов;
- произвольные конфигурации — можно указать любое соотношение ресурсов.

Используемые процессоры зависят от выбранной конфигурации.

Около 5 ГБ локального диска во всех конфигурациях зарезервировано под операционную систему, компоненты сервиса и хранение логов. Остальной объем доступен для размещения баз данных.

После создания кластера можно изменить конфигурацию нод.

Процессоры

В линейках фиксированных конфигураций и произвольных конфигураций различаются доступные процессоры. Частота процессора влияет на скорость обработки запросов пользователей, выполнения сложных алгоритмов и операций с данными.

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

	Фиксированные конфигурации Standard, CPU, Memory	**Фиксированные конфигурации HighFreq**	**Фиксированные конфигурации Dedicated**	**Произвольные конфигурации**
Процессор	Intel® Xeon® Scalable, AMD EPYC™	Intel® Xeon® Gold 6354	Intel® Xeon® Gold 6240	Intel® Xeon® Scalable, AMD EPYC™

Частота процессора	2,2—2,4 ГГц	3,00 ГГц \Режим Turbo Boost 3,60 ГГц*	2,6 ГГц \Режим Turbo Boost 3,9 ГГц*	2,2—2,4 ГГц

* При нагрузке облачного сервера в 100% процессор работает с технологией Turbo Boost и максимальной частотой 3,6 ГГц для линейки HighFreq и 3,9 ГГц для линейки Dedicated. Так как процессор эмулируется, при тестировании будет отображаться частота 3,00 ГГц для линейки HighFreq и 2,6 ГГц для линейки Dedicated.

Фиксированные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

Фиксированную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Standard

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM, подходит для большинства СУБД. Рекомендуем использовать эту линейку, если вы не знаете профиль нагрузки.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
4	16 ГБ	128 ГБ
6	32 ГБ	256 ГБ
8	64 ГБ	512 ГБ
10	96 ГБ	768 ГБ
12	128 ГБ	1 ТБ
16	160 ГБ	1,5 ТБ
20	208 ГБ	2 ТБ

CPU

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к вычислениям. Например,

если в базе данных выполняются аналитические запросы, множественные вложенные запросы или шифрование данных. Один из способов определить такой профиль нагрузки — отслеживать метрику `Load Average`, которая показывает среднее значение загрузки системы за одну, пять или 15 минут.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
6	16 ГБ	128 ГБ
8	32 ГБ	256 ГБ
10	64 ГБ	512 ГБ
12	96 ГБ	768 ГБ
16	128 ГБ	1 ТБ
20	160 ГБ	1,5 ТБ
24	208 ГБ	2 ТБ

Memory

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к кэшированию. Например, если в базе данных выполняются множественные, редкоповторяющиеся запросы к различным частям таблиц. Один из способов определить такой профиль нагрузки — отслеживать метрику `Попадание в кэш (Cash_hit_ratio)`, которая показывает процент данных в запросе, которые прочитаны из кэша.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
2	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ

10	128 ГБ	1 ТБ
14	160 ГБ	1,5 ТБ
16	208 ГБ	2 ТБ

HighFreq

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM.

Используется высокопроизводительное оборудование Enterprise-уровня:

- процессоры Intel® Xeon® Gold 6354 с частотой в режиме Turbo Boost до 3,6 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM ECC Reg 3,2 ГГц;
- SSD NVMe-диски повышенной производительности.

Количество vCPU	**RAM**	**Диск**
4	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	32 ГБ	256 ГБ
8	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	64 ГБ	512 ГБ
10	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ
10	96 ГБ	768 ГБ
12	96 ГБ	768 ГБ
10	120 ГБ	962 ГБ
12	120 ГБ	962 ГБ
14	120 ГБ	962 ГБ
12	152 ГБ	1,22 ТБ

14	152 ГБ	1,22 ТБ
16	184 ГБ	1,5 ТБ

Dedicated

Линейка фиксированных конфигураций с нодами кластера на отдельных облачных серверах. Каждый облачный сервер занимает весь выделенный хост (физический сервер). Подходит для пользователей, которым необходима физическая изоляция баз данных от других клиентов, максимальная производительность и максимальные размеры доступных ресурсов.

Используется высокопроизводительное оборудование Enterprise-уровня:

- один процессор Intel® Xeon® Gold 6240 с частотой в режиме Turbo Boost до 3,9 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM 64 ГБ DDR4 ECC Reg;
- два SSD NVMe-диска в RAID 1;
- две сетевые карты 2 × 25 GE для основной сети + MC-LAG со скоростью подключения 25 Гбит/с для сервисной сети (для резервного копирования, мониторинга, репликации данных в кластере).

	Количество vCPU	**RAM**	**Диск**
Medium	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 5 x 64 ГБ Физически на сервере 6 x 64 ГБ**	Доступно для СУБД 3,4 ТБ Физически на сервере 2 x 4 ТБ***
Large	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 7 x 64 ГБ Физически на сервере 8 x 64 ГБ**	Доступно для СУБД 7,2 ТБ Физически на сервере 2 x 8 ТБ***

* Чтобы повысить производительность кластера СУБД, используется технология гиперпоточности (Hyper-Threading Technology). Эта технология позволяет использовать 34 vCPU на базе физических 18 CPU. Такая производительность подойдет для высоконагруженных систем или аналитического профиля нагрузки.

** Одна планка оперативной памяти зарезервирована для сервисных служб, которые обслуживают физический сервер.

*** Чтобы обеспечить дополнительную отказоустойчивость, диски размещены в RAID 1. Это массив дисков с зеркалированием, поэтому для базы данных доступно 50% дискового пространства. Часть дискового пространства также зарезервировано для сервисных служб, которые обслуживают физический сервер.

Произвольные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

В произвольных конфигурациях используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Произвольную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Значения произвольных конфигураций

В произвольных конфигурациях можно выбрать соотношение ресурсов. При выборе конфигурации учтите:

- соотношение vCPU:RAM должно быть не менее, чем 1:4. Например, для 4 vCPU нужно не менее 16 ГБ RAM;
- соотношение vCPU:Локальный диск должно быть не менее, чем 1:32. Например, для 4 vCPU нужен диск размером не менее 128 ГБ.

Доступные значения зависят от пула.

	В пулах ru-1, ru-2, gis-1, uz-1, kz-1, ke-1	**В пулах ru-3, ru-9, ru-7, ru-8**
Количество vCPU	1—8	1—32
RAM	4—64 ГБ	4—256 ГБ
Размер локального диска	32—512 ГБ	32 ГБ — 1,23 ТБ

Создать кластер PostgreSQL

1. В панели управления перейдите в раздел **Облачная платформа** → **Базы данных**.
2. Нажмите **Создать кластер**.
3. Введите имя кластера.
4. Выберите регион.

5. Выберите пул.
6. Выберите версию PostgreSQL. После создания версию будет нельзя изменить.
7. Выберите конфигурацию нод:
    - фиксированная — конфигурации с разным соотношением vCPU, RAM и локального диска;
    - произвольная — свободный выбор соотношения ресурсов.
8. Для фиксированной конфигурации выберите линейку конфигурации:
    - Standard;
    - CPU;
    - Memory;
    - HighFreq;
    - Dedicated.
9. Опционально: отметьте чекбокс **Добавить реплики** и укажите количество реплик. Реплики повышают отказоустойчивость кластера.
10. Выберите тип подсети, к которой будет подключен кластер:
    - приватная подсеть — подсеть без доступа из интернета. Можно подключить статический публичный IP-адрес;
    - публичная подсеть — все адреса публичной подсети доступны из интернета.
11. Выберите или создайте подсеть.
    Адреса присваиваются каждой ноде в кластере. Убедитесь, что количество адресов в подсети не меньше количества нод в кластере. Если после создания кластера вы планируете увеличить количество реплик, то выберите подсеть, в которой есть запас свободных адресов. После создания кластера подсеть нельзя изменить.
    Вы можете ограничить список адресов, с которых будет разрешен доступ в кластер баз данных.
12. Опционально: в приватной подсети вы можете подключить публичный IP-адрес к ноде кластера:
    - если вы выбрали существующую приватную подсеть — отметьте чекбокс **Публичный доступ к нодам кластера**, а затем чекбокс той ноды, к которой нужно предоставить публичный доступ. Приватная подсеть должна соответствовать требованиям;
    - если вы создаете новую приватную подсеть — подключите публичный IP-адрес после создания кластера.
13. Выберите режим пулера соединений:
    - transaction — соединение назначено на клиента на время транзакции;
    - session — соединение назначено, пока клиент подключен;
    - statement — транзакции с несколькими операторами запрещены.
14. Выберите размер пула.
15. Опционально: измените настройки СУБД, для этого нажмите **Изменить**. Мы рекомендуем менять значения настроек только при необходимости — неправильно подобранные значения могут снизить производительность кластера.
16. Нажмите **Создать кластер баз данных**. Кластер будет готов к работе, когда перейдет в статус `ACTIVE`.

Создать базу данных

1. Создайте пользователя — у базы данных должен быть пользователь-владелец.
2. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
3. Откройте страницу кластера → вкладка **Базы данных**.
4. Нажмите **Создать базу данных**.
5. Введите имя базы данных.
6. Выберите пользователя-владельца базы данных.
7. Введите локаль набора символов (LC_CTYPE) — отвечает за классификацию символов и различия в их регистре. После создания базы данных изменить локаль нельзя. Подробнее о локалях в документации PostgreSQL.
8. Введите локаль сортировки (LC_COLLATE) — определяет настройки сравнения строк и символов, а также влияет на сортировку. После создания базы данных изменить локаль нельзя.
9. Нажмите **Создать**.

Расширения PostgreSQL

К базам данных PostgreSQL можно подключать расширения. Расширения позволяют добавлять функциональности к базе данных без изменения исходного кода самой СУБД.

Список расширений доступных в облачных базах данных можно посмотреть в таблице Описание расширений.

Некоторые расширения зависят от других — зависимые расширения не будут работать без главного расширения. Список зависимых и главных расширений можно посмотреть в таблице Зависимые расширения.

Добавить расширение можно в панели управления, через API Облачных баз данных и через Terraform.

Добавить расширение

Расширения подключаются отдельно к каждой базе данных. Если вы подключаете зависимое расширение и главное расширение ещё не подключено, то сначала автоматически будет подключено главное расширение, а потом зависимое.

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Откройте страницу кластера → вкладка **Базы данных** → карточка базы данных.
3. В блоке **Расширения** нажмите **Добавить расширение**.
4. Выберите расширение. Список доступных расширений и их описание можно посмотреть в таблице Описание расширений.
5. Нажмите **Добавить**.

Удалить расширение

Зависимое расширение можно удалить отдельно. Чтобы удалить главное расширение, сначала удалите зависимое. Список зависимых и главных расширений можно посмотреть в таблице Зависимые расширения.

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Откройте страницу кластера → вкладка **Базы данных** → карточка базы данных.
3. В блоке **Расширения**, в строке расширения нажмите 🗑️.

Описание расширений

address_standardizer	Используется для структурирования почтовых адресов, переданных в виде строки
address_standardizer_data_us	Используется для структурирования почтовых адресов США и Канады для расширения `address_standardizer`
autoinc	Содержит функцию `autoinc()`. Эта функция возвращает следующее значение для последовательности, которое хранится в поле целочисленного типа. В отличие от встроенных типов, управляющих последовательностями, `autoinc()`: • блокирует попытки вставить в поле значение из запроса; • позволяет изменять значение в поле при обновлении записи
bloom	Добавляет доступ к индексам баз данных на основе фильтров Блума, которые требуют значительно меньше памяти, чем хеш-таблицы, но допускают ложноположительные срабатывания
btree_gin	Содержит примеры классов оператора GIN (Generalized Inverted Index, обобщенный инвертированный индекс), который используется для обратного поиска

btree_gist	Содержит классы оператора GiST (Generalized Search Tree, обобщенное дерево поиска). В отличие от индексов B-tree, GiST поддерживает операторы <> (не равно) и < — > (дистанция), хотя и не обеспечивает уникальности возвращаемых значений
citext	Содержит тип данных `citext`, который используется для регистронезависимой работы со строками
cube	Содержит тип данных `cube`, который используется для представления многомерных кубов
dict_int	Содержит пример дополнительного шаблона словаря для полнотекстового поиска, с помощью которого можно избежать разрастания списка уникальных слов и увеличить скорость поиска
dict_xsyn	Содержит пример дополнительного шаблона словаря синонимов (Extended Synonym Dictionary) для полнотекстового поиска: при поиске слова будут найдены все его синонимы
fuzzystrmatch	Содержит функции, которые используются для определения сходства и различия строк
hstore	Содержит тип `hstore`, который позволяет хранить пары ключ/значение в одном поле таблицы и эффективно работать с ними
intarray	Содержит функции и операторы для работы с массивами целых чисел, в которых нет пустых (NULL) значений
ip4r	Поддерживает индексацию IPv4 и IPv6 адресов для повышения производительности запросов

isn	Содержит типы данных для международных стандартов нумерации продукции EAN13, UPC, ISBN, ISMN и ISSN. Проверка и формирование номеров осуществляется по заданному списку префиксов
jsquery	Добавляет поддержку языка JsQuery, который используется для работы с данными типа `jsonb`. JsQuery позволяет организовать эффективный поиск во вложенных объектах и содержит дополнительные операторы сравнения с поддержкой индексов
lo	Содержит тип данных `lo` и функцию `lo_manage()`, которые используются для управления большими бинарными объектами (Binary Large Object, BLOB) в соответствии с требованиями спецификаций драйверов JDBC и ODBC (стандартное поведение PostgreSQL им не соответствует)
ltree	Содержит тип данных `ltree` для представления меток данных, хранящихся в древовидной иерархической структуре
moddatetime	Содержит функцию `moddatetime()`, которая позволяет отслеживать время последней модификации строки таблицы
pg_partman	Добавляет расширенные возможности по партицированию таблиц, в том числе на основе времени или последовательности

pg_stat_statements	Добавляет возможности отслеживания планирования и сбора статистики выполнения всех SQL-запросов, запущенных в кластере. Для использования расширения необходима роль `dbaas_admin` — эта роль автоматически выдается владельцу базы данных, назначить ее другим пользователям нельзя
pgtrgm	Содержит инструменты для быстрого поиска похожих строк на основе сопоставления триграмм
pgcrypto	Предоставляет набор криптографических функций для защиты данных. Подробнее о шифровании данных с помощью расширения pgcrypto и примеры использования в инструкции Шифрование данных
pgrowlocks	Содержит функцию `pgrowlocks()`, которая возвращает сведения о блокировке строк в указанной таблице
pgTAP	Предоставляет набор инструментов для тестирования схемы базы данных и SQL-функций
plv8	Позволяет использовать JavaScript для написания хранимых процедур и триггеров
postgis	Позволяет хранить и обрабатывать объекты геоинформационных систем (ГИС) в базах данных PostgreSQL. Для использования расширения необходима роль `dbaas_admin` — эта роль автоматически выдается владельцу базы данных, назначить ее другим пользователям нельзя

postgis_raster	Позволяет работать с растровыми изображениями и проводить анализ объектов геоинформационных систем (ГИС) в базах данных
postgis_fdw	Добавляет поддержку Foreign Data Wrapper, чтобы получить доступ к внешним серверам PostgreSQL. Для использования расширения необходима роль `dbaas_admin` — эта роль автоматически выдается владельцу базы данных, назначить ее другим пользователям нельзя
prefix	Добавляет поддержку префиксов и масок для оптимизации запросов
rum	Добавляет метод доступа для работы с индексами RUM
seg	Содержит тип данных `seg` для представления отрезков линий или интервалов с плавающей запятой
tablefunc	Содержит набор функций, возвращающих таблицы (наборы строк)
unaccent	Содержит словарь для поиска текста без учета диакритических знаков
uuid-ossp	Содержит функции для генерации UUID по стандартным алгоритмам
xml2	Добавляет поддержку запросов XPath и языка XSLT

Зависимые расширения

earthdistance	Содержит модуль для вычисления расстояний между точками на поверхности Земли. Работает только вместе с главным расширением `cube`

pg_stat_kcache	Добавляет возможность сбора статистики по операциям чтения и записи, выполненным на уровне файловой системы. Работает только вместе с главным расширением `pg_stat_statements`. Для использования расширения необходима роль `dbaas_admin` — эта роль автоматически выдается владельцу базы данных, назначить ее другим пользователям нельзя
pgrouting	Содержит функции для геопространственной маршрутизации базы данных PostGIS. Работает только вместе с главным расширением `postgis`
postgis_tiger_geocoder	Содержит функции для геокодирования на основе данных в формате `TIGER`. Работает только вместе с главным расширением `postgis`
postgis_topology	Содержит типы данных и функции расширения `postgis` для управления топологическими объектами. Работает только вместе с главным расширением `postgis`. Для использования расширения необходима роль `dbaas_admin` — эта роль автоматически выдается владельцу базы данных, назначить ее другим пользователям нельзя

PostgreSQL для 1С

Версии и конфигурации PostgreSQL для 1С

Версии

Поддерживаются версии PostgreSQL для 1С 12, 13 и 14.

Конфигурации нод

При создании кластера облачных баз данных PostgreSQL для 1С можно выбрать для нод количество vCPU, RAM и размер локального диска.

Доступно два типа конфигураций:

- фиксированные конфигурации — несколько линеек с разными техническими характеристиками, в которых зафиксировано соотношение ресурсов;
- произвольные конфигурации — можно указать любое соотношение ресурсов.

Используемые процессоры зависят от выбранной конфигурации.

Около 5 ГБ локального диска во всех конфигурациях зарезервировано под операционную систему, компоненты сервиса и хранение логов. Остальной объем доступен для размещения баз данных.

После создания кластера можно изменить конфигурацию нод.

Процессоры

В линейках фиксированных конфигураций и произвольных конфигураций различаются доступные процессоры. Частота процессора влияет на скорость обработки запросов пользователей, выполнения сложных алгоритмов и операций с данными.

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

	Фиксированные конфигурации Standard, CPU, Memory	**Фиксированные конфигурации HighFreq**	**Фиксированные конфигурации Dedicated**	**Произвольные конфигурации**
Процессор	Intel® Xeon® Scalable, AMD EPYC™	Intel® Xeon® Gold 6354	Intel® Xeon® Gold 6240	Intel® Xeon® Scalable, AMD EPYC™

Частота процессора	2,2—2,4 ГГц	3,00 ГГц \Режим Turbo Boost 3,60 ГГц*	2,6 ГГц \Режим Turbo Boost 3,9 ГГц*	2,2—2,4 ГГц

* При нагрузке облачного сервера в 100% процессор работает с технологией Turbo Boost и максимальной частотой 3,6 ГГц для линейки HighFreq и 3,9 ГГц для линейки Dedicated. Так как процессор эмулируется, при тестировании будет отображаться частота 3,00 ГГц для линейки HighFreq и 2,6 ГГц для линейки Dedicated.

Фиксированные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

Фиксированную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Standard

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM, подходит для большинства СУБД. Рекомендуем использовать эту линейку, если вы не знаете профиль нагрузки.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
4	16 ГБ	128 ГБ
6	32 ГБ	256 ГБ
8	64 ГБ	512 ГБ
10	96 ГБ	768 ГБ
12	128 ГБ	1 ТБ
16	160 ГБ	1,5 ТБ
20	208 ГБ	2 ТБ

CPU

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к вычислениям. Например,

если в базе данных выполняются аналитические запросы, множественные вложенные запросы или шифрование данных. Один из способов определить такой профиль нагрузки — отслеживать метрику `Load Average`, которая показывает среднее значение загрузки системы за одну, пять или 15 минут.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
6	16 ГБ	128 ГБ
8	32 ГБ	256 ГБ
10	64 ГБ	512 ГБ
12	96 ГБ	768 ГБ
16	128 ГБ	1 ТБ
20	160 ГБ	1,5 ТБ
24	208 ГБ	2 ТБ

Memory

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к кэшированию. Например, если в базе данных выполняются множественные, редкоповторяющиеся запросы к различным частям таблиц. Один из способов определить такой профиль нагрузки — отслеживать метрику `Попадание в кэш (Cash_hit_ratio)`, которая показывает процент данных в запросе, которые прочитаны из кэша.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
2	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ

10	128 ГБ	1 ТБ
14	160 ГБ	1,5 ТБ
16	208 ГБ	2 ТБ

HighFreq

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM.

Используется высокопроизводительное оборудование Enterprise-уровня:

- процессоры Intel® Xeon® Gold 6354 с частотой в режиме Turbo Boost до 3,6 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM ECC Reg 3,2 ГГц;
- SSD NVMe-диски повышенной производительности.

Количество vCPU	**RAM**	**Диск**
4	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	32 ГБ	256 ГБ
8	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	64 ГБ	512 ГБ
10	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ
10	96 ГБ	768 ГБ
12	96 ГБ	768 ГБ
10	120 ГБ	962 ГБ
12	120 ГБ	962 ГБ
14	120 ГБ	962 ГБ
12	152 ГБ	1,22 ТБ

14	152 ГБ	1,22 ТБ
16	184 ГБ	1,5 ТБ

Dedicated

Линейка фиксированных конфигураций с нодами кластера на отдельных облачных серверах. Каждый облачный сервер занимает весь выделенный хост (физический сервер). Подходит для пользователей, которым необходима физическая изоляция баз данных от других клиентов, максимальная производительность и максимальные размеры доступных ресурсов.

Используется высокопроизводительное оборудование Enterprise-уровня:

- один процессор Intel® Xeon® Gold 6240 с частотой в режиме Turbo Boost до 3,9 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM 64 ГБ DDR4 ECC Reg;
- два SSD NVMe-диска в RAID 1;
- две сетевые карты 2 × 25 GE для основной сети + MC-LAG со скоростью подключения 25 Гбит/с для сервисной сети (для резервного копирования, мониторинга, репликации данных в кластере).

	Количество vCPU	**RAM**	**Диск**
Medium	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 5 x 64 ГБ Физически на сервере 6 x 64 ГБ**	Доступно для СУБД 3,4 ТБ Физически на сервере 2 x 4 ТБ***
Large	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 7 x 64 ГБ Физически на сервере 8 x 64 ГБ**	Доступно для СУБД 7,2 ТБ Физически на сервере 2 x 8 ТБ***

* Чтобы повысить производительность кластера СУБД, используется технология гиперпоточности (Hyper-Threading Technology). Эта технология позволяет использовать 34 vCPU на базе физических 18 CPU. Такая производительность подойдет для высоконагруженных систем или аналитического профиля нагрузки.

** Одна планка оперативной памяти зарезервирована для сервисных служб, которые обслуживают физический сервер.

*** Чтобы обеспечить дополнительную отказоустойчивость, диски размещены в RAID 1. Это массив дисков с зеркалированием, поэтому для базы данных доступно 50% дискового пространства. Часть дискового пространства также зарезервировано для сервисных служб, которые обслуживают физический сервер.

Произвольные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

В произвольных конфигурациях используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Произвольную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Значения произвольных конфигураций

В произвольных конфигурациях можно выбрать соотношение ресурсов. При выборе конфигурации учтите:

- соотношение vCPU:RAM должно быть не менее, чем 1:4. Например, для 4 vCPU нужно не менее 16 ГБ RAM;
- соотношение vCPU:Локальный диск должно быть не менее, чем 1:32. Например, для 4 vCPU нужен диск размером не менее 128 ГБ.

Доступные значения зависят от пула.

	В пулах ru-1, ru-2, gis-1, uz-1, kz-1, ke-1	**В пулах ru-3, ru-9, ru-7, ru-8**
Количество vCPU	1—8	1—32
RAM	4—64 ГБ	4—256 ГБ
Размер локального диска	32—512 ГБ	32 ГБ — 1,23 ТБ

Создать кластер PostgreSQL для 1С

В облачных базах данных вы можете создать кластер PostgreSQL, настроенный специально для работы с 1С:Предприятие.

1. В панели управления перейдите в раздел **Облачная платформа** → **Базы данных**.

2. Нажмите **Создать кластер**.

3. Введите имя кластера.

4. Выберите регион.

5. Выберите пул.

6. Выберите версию PostgreSQL для 1С.

7. Выберите конфигурацию нод:

    - фиксированная — конфигурации с разным соотношением vCPU, RAM и локального диска;
    - произвольная — свободный выбор соотношения ресурсов.

8. Выбор конфигурации зависит от количества пользователей, которые одновременно работают с 1С, и от размера информационной базы. Например, если в 1С одновременно работают до 50 пользователей, то подойдет конфигурация с 4 vCPU и 16 ГБ RAM. Если более 50 пользователей, то мы рекомендуем конфигурацию 8 vCPU и 32 ГБ RAM.

9. Для фиксированной конфигурации выберите линейку конфигурации:

    - Standard;
    - CPU;
    - Memory;
    - HighFreq;
    - Dedicated.

10. Опционально: отметьте чекбокс **Добавить реплики** и укажите количество реплик. Реплики повышают отказоустойчивость кластера.

11. Выберите тип подсети, к которой будет подключен кластер:

    - приватная подсеть — подсеть без доступа из интернета. Можно подключить статический публичный IP-адрес;
    - публичная подсеть — все адреса публичной подсети доступны из интернета.

12. Выберите или создайте подсеть.

    Адреса присваиваются каждой ноде в кластере. Убедитесь, что количество адресов в подсети не меньше количества нод в кластере. Если после создания кластера вы планируете увеличить количество реплик, то выберите подсеть, в которой есть запас свободных адресов. После создания кластера подсеть нельзя изменить.

    Вы можете ограничить список адресов, с которых будет разрешен доступ в кластер баз данных.

13. Опционально: в приватной подсети вы можете подключить публичный IP-адрес к ноде кластера:

    - если вы выбрали существующую приватную подсеть — отметьте чекбокс **Публичный доступ к нодам кластера**, а затем чекбокс той ноды, к которой нужно предоставить публичный доступ. Приватная подсеть должна соответствовать требованиям;
    - если вы создаете новую приватную подсеть — подключите публичный IP-адрес после создания кластера.
14. Опционально: измените настройки СУБД, для этого нажмите **Изменить**. Мы рекомендуем менять значения настроек только при необходимости — неправильно подобранные значения могут снизить производительность кластера.

15. Нажмите **Создать кластер баз данных**.

16. Создайте базу данных.

Создать базу данных

1. Создайте пользователя — у базы данных должен быть пользователь-владелец.
2. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
3. Откройте страницу кластера → вкладка **Базы данных**.
4. Нажмите **Создать базу данных**.
5. Введите имя базы данных.
6. Выберите пользователя-владельца базы данных.
7. Введите локаль набора символов (LC_CTYPE) — отвечает за классификацию символов и различия в их регистре. После создания базы данных изменить локаль нельзя. Подробнее о локалях в документации PostgreSQL.
8. Введите локаль сортировки (LC_COLLATE) — определяет настройки сравнения строк и символов, а также влияет на сортировку. После создания базы данных изменить локаль нельзя.
9. Нажмите **Создать**.

Подключить базу данных к серверу 1С

Чтобы подключить базу данных PostgreSQL как информационную базу 1С, в форме добавления информационной базы в 1С:Предприятие используйте параметры:

- Защищенное соединение — **Выключено**;
- Тип СУБД — **PostgreSQL**;
- Сервер баз данных — **<DNS-адрес мастер-ноды> port:5432**;
- Имя базы данных — **Имя созданной базы данных**;
- Пользователь базы данных — **Имя пользователя**;
- Пароль пользователя — **Пароль**.

Настройки PostgreSQL для 1С

Настройки PostgreSQL влияют на производительность кластера баз данных. При создании кластера баз данных PostgreSQL значения для всех настроек задаются автоматически. Значения подобраны так, чтобы обеспечить высокую производительность кластера, они отличаются в зависимости от конфигурации кластера и версии PostgreSQL.

Если автоматические значения не подходят для ваших задач, установите свои значения при создании кластера или измените настройки в уже созданном кластере.

Мы рекомендуем менять значения настроек только при необходимости — неправильно подобранные значения могут снизить производительность кластера. При масштабировании кластера значения некоторых настроек автоматически заменяются на допустимые.

Посмотреть список настроек

Посмотрите подробное описание настроек в официальной документации PostgreSQL.

Посмотреть список настроек, доступных для изменения, можно при создании кластера или изменении настроек.

Если вы изменили настройки, вы можете посмотреть список всех изменений.

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Откройте страницу кластера → вкладка **Настройки**.
3. В блоке **Настройки СУБД** отображены измененные ранее настройки — название и значение.

Изменить настройки

Изменение некоторых параметров в настройках влечет за собой перезагрузку баз данных в кластере — кластер в это время может быть недоступен. Посмотрите список этих настроек.

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Откройте страницу кластера → вкладка **Настройки**.
3. В блоке **Настройки СУБД** нажмите **Изменить** и укажите новые значения.
4. Нажмите **Сохранить**

Список настроек, которые требуют перезагрузки

- autovacuum_freeze_max_age;
- autovacuum_max_workers;
- autovacuum_multixact_freeze_max_age;
- max_files_per_process;
- max_pred_locks_per_transaction;
- max_prepared_transactions;
- old_snapshot_threshold;

- track_activity_query_size;
- max_connections;
- max_locks_per_transaction;
- max_worker_processes;
- shared_buffers.

Настройки при масштабировании кластера

У любого параметра СУБД есть границы допустимых значений. При масштабировании кластера (изменении конфигурации) значения некоторых настроек автоматически заменяются на допустимые, чтобы кластер мог работать.

Когда кластер будет масштабирован и перейдет в статус `ACTIVE`, вы сможете установить новые значения — изменить настройки.

Список настроек, которые меняют значения при масштабировании кластера:

- `shared_buffers`;
- `effective_cache_size`;
- `maintenance_work_mem`;
- `max_worker_processes`;
- `max_parallel_workers`;
- `autovacuum_max_workers`;
- `vacuum_cost_limit`;
- `max_parallel_workers_per_gather`;
- `max_maintenance_workers`.

PostgreSQL TimescaleDB

Версии и конфигурации PostgreSQL TimescaleDB

Версии

Поддерживаются версии PostgreSQL 12, 13, 14, 15 и 16. Для каждой из версий PostgreSQL мы устанавливаем последнюю доступную версию TimescaleDB. Расширение TimescaleDB распространяется по лицензии Apache 2.0.

Конфигурации нод

При создании кластера облачных баз данных PostgreSQL TimescaleDB можно выбрать для нод количество vCPU, RAM и размер локального диска.

Доступно два типа конфигураций:

- фиксированные конфигурации — несколько линеек с разными техническими характеристиками, в которых зафиксировано соотношение ресурсов;
- произвольные конфигурации — можно указать любое соотношение ресурсов.

Используемые процессоры зависят от выбранной конфигурации.

Около 5 ГБ локального диска во всех конфигурациях зарезервировано под операционную систему, компоненты сервиса и хранение логов. Остальной объем доступен для размещения баз данных.

После создания кластера можно изменить конфигурацию нод.

Процессоры

В линейках фиксированных конфигураций и произвольных конфигураций различаются доступные процессоры. Частота процессора влияет на скорость обработки запросов пользователей, выполнения сложных алгоритмов и операций с данными.

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

	Фиксированные конфигурации Standard, CPU, Memory	**Фиксированные конфигурации HighFreq**	**Фиксированные конфигурации Dedicated**	**Произвольные конфигурации**
Процессор	Intel® Xeon® Scalable, AMD EPYC™	Intel® Xeon® Gold 6354	Intel® Xeon® Gold 6240	Intel® Xeon® Scalable, AMD EPYC™

Частота процессора	2,2—2,4 ГГц	3,00 ГГц \Режим Turbo Boost 3,60 ГГц*	2,6 ГГц \Режим Turbo Boost 3,9 ГГц*	2,2—2,4 ГГц

* При нагрузке облачного сервера в 100% процессор работает с технологией Turbo Boost и максимальной частотой 3,6 ГГц для линейки HighFreq и 3,9 ГГц для линейки Dedicated. Так как процессор эмулируется, при тестировании будет отображаться частота 3,00 ГГц для линейки HighFreq и 2,6 ГГц для линейки Dedicated.

Фиксированные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

Фиксированную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Standard

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM, подходит для большинства СУБД. Рекомендуем использовать эту линейку, если вы не знаете профиль нагрузки.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
4	16 ГБ	128 ГБ
6	32 ГБ	256 ГБ
8	64 ГБ	512 ГБ
10	96 ГБ	768 ГБ
12	128 ГБ	1 ТБ
16	160 ГБ	1,5 ТБ
20	208 ГБ	2 ТБ

CPU

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к вычислениям. Например,

если в базе данных выполняются аналитические запросы, множественные вложенные запросы или шифрование данных. Один из способов определить такой профиль нагрузки — отслеживать метрику `Load Average`, которая показывает среднее значение загрузки системы за одну, пять или 15 минут.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
6	16 ГБ	128 ГБ
8	32 ГБ	256 ГБ
10	64 ГБ	512 ГБ
12	96 ГБ	768 ГБ
16	128 ГБ	1 ТБ
20	160 ГБ	1,5 ТБ
24	208 ГБ	2 ТБ

Memory

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к кэшированию. Например, если в базе данных выполняются множественные, редкоповторяющиеся запросы к различным частям таблиц. Один из способов определить такой профиль нагрузки — отслеживать метрику `Попадание в кэш (Cash_hit_ratio)`, которая показывает процент данных в запросе, которые прочитаны из кэша.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
2	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ

10	128 ГБ	1 ТБ
14	160 ГБ	1,5 ТБ
16	208 ГБ	2 ТБ

HighFreq

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM.

Используется высокопроизводительное оборудование Enterprise-уровня:

- процессоры Intel® Xeon® Gold 6354 с частотой в режиме Turbo Boost до 3,6 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM ECC Reg 3,2 ГГц;
- SSD NVMe-диски повышенной производительности.

Количество vCPU	**RAM**	**Диск**
4	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	32 ГБ	256 ГБ
8	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	64 ГБ	512 ГБ
10	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ
10	96 ГБ	768 ГБ
12	96 ГБ	768 ГБ
10	120 ГБ	962 ГБ
12	120 ГБ	962 ГБ
14	120 ГБ	962 ГБ
12	152 ГБ	1,22 ТБ

14	152 ГБ	1,22 ТБ
16	184 ГБ	1,5 ТБ

Dedicated

Линейка фиксированных конфигураций с нодами кластера на отдельных облачных серверах. Каждый облачный сервер занимает весь выделенный хост (физический сервер). Подходит для пользователей, которым необходима физическая изоляция баз данных от других клиентов, максимальная производительность и максимальные размеры доступных ресурсов.

Используется высокопроизводительное оборудование Enterprise-уровня:

- один процессор Intel® Xeon® Gold 6240 с частотой в режиме Turbo Boost до 3,9 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM 64 ГБ DDR4 ECC Reg;
- два SSD NVMe-диска в RAID 1;
- две сетевые карты 2 × 25 GE для основной сети + MC-LAG со скоростью подключения 25 Гбит/с для сервисной сети (для резервного копирования, мониторинга, репликации данных в кластере).

	Количество vCPU	**RAM**	**Диск**
Medium	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 5 x 64 ГБ Физически на сервере 6 x 64 ГБ**	Доступно для СУБД 3,4 ТБ Физически на сервере 2 x 4 ТБ***
Large	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 7 x 64 ГБ Физически на сервере 8 x 64 ГБ**	Доступно для СУБД 7,2 ТБ Физически на сервере 2 x 8 ТБ***

* Чтобы повысить производительность кластера СУБД, используется технология гиперпоточности (Hyper-Threading Technology). Эта технология позволяет использовать 34 vCPU на базе физических 18 CPU. Такая производительность подойдет для высоконагруженных систем или аналитического профиля нагрузки.

** Одна планка оперативной памяти зарезервирована для сервисных служб, которые обслуживают физический сервер.

*** Чтобы обеспечить дополнительную отказоустойчивость, диски размещены в RAID 1. Это массив дисков с зеркалированием, поэтому для базы данных доступно 50% дискового пространства. Часть дискового пространства также зарезервировано для сервисных служб, которые обслуживают физический сервер.

Произвольные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

В произвольных конфигурациях используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Произвольную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Значения произвольных конфигураций

В произвольных конфигурациях можно выбрать соотношение ресурсов. При выборе конфигурации учтите:

- соотношение vCPU:RAM должно быть не менее, чем 1:4. Например, для 4 vCPU нужно не менее 16 ГБ RAM;
- соотношение vCPU:Локальный диск должно быть не менее, чем 1:32. Например, для 4 vCPU нужен диск размером не менее 128 ГБ.

Доступные значения зависят от пула.

	В пулах ru-1, ru-2, gis-1, uz-1, kz-1, ke-1	**В пулах ru-3, ru-9, ru-7, ru-8**
Количество vCPU	1—8	1—32
RAM	4—64 ГБ	4—256 ГБ
Размер локального диска	32—512 ГБ	32 ГБ — 1,23 ТБ

Создать кластер PostgreSQL TimescaleDB

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Нажмите **Создать кластер**.
3. Введите имя кластера.

4. Выберите регион.
5. Выберите пул.
6. Выберите версию PostgreSQL TimescaleDB. После создания версию будет нельзя изменить.
7. Выберите конфигурацию нод:
    - фиксированная — конфигурации с разным соотношением vCPU, RAM и локального диска;
    - произвольная — свободный выбор соотношения ресурсов.
8. Для фиксированной конфигурации выберите линейку конфигурации:
    - Standard;
    - CPU;
    - Memory;
    - HighFreq;
    - Dedicated.
9. Опционально: отметьте чекбокс **Добавить реплики** и укажите количество реплик. Реплики повышают отказоустойчивость кластера.
10. Выберите тип подсети, к которой будет подключен кластер:
    - приватная подсеть — подсеть без доступа из интернета. Можно подключить статический публичный IP-адрес;
    - публичная подсеть — все адреса публичной подсети доступны из интернета.
11. Выберите или создайте подсеть.
    Адреса присваиваются каждой ноде в кластере. Убедитесь, что количество адресов в подсети не меньше количества нод в кластере. Если после создания кластера вы планируете увеличить количество реплик, то выберите подсеть, в которой есть запас свободных адресов. После создания кластера подсеть нельзя изменить.
    Вы можете ограничить список адресов, с которых будет разрешен доступ в кластер баз данных.
12. Опционально: в приватной подсети вы можете подключить публичный IP-адрес к ноде кластера:
    - если вы выбрали существующую приватную подсеть — отметьте чекбокс **Публичный доступ к нодам кластера**, а затем чекбокс той ноды, к которой нужно предоставить публичный доступ. Приватная подсеть должна соответствовать требованиям;
    - если вы создаете новую приватную подсеть — подключите публичный IP-адрес после создания кластера.
13. Выберите режим пулера соединений:
    - transaction — соединение назначено на клиента на время транзакции;
    - session — соединение назначено, пока клиент подключен;
    - statement — транзакции с несколькими операторами запрещены.
14. Выберите размер пула.
15. Опционально: измените настройки СУБД, для этого нажмите **Изменить**. Мы рекомендуем менять значения настроек только при необходимости — неправильно подобранные значения могут снизить производительность кластера.
16. Нажмите **Создать кластер баз данных**. Кластер будет готов к работе, когда перейдет в статус `ACTIVE`.

Создать базу данных

1. Создайте пользователя — у базы данных должен быть пользователь-владелец.
2. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
3. Откройте страницу кластера → вкладка **Базы данных**.
4. Нажмите **Создать базу данных**.
5. Введите имя базы данных.
6. Выберите пользователя-владельца базы данных.
7. Введите локаль набора символов (LC_CTYPE) — отвечает за классификацию символов и различия в их регистре. После создания базы данных изменить локаль нельзя. Подробнее о локалях в документации PostgreSQL.
8. Введите локаль сортировки (LC_COLLATE) — определяет настройки сравнения строк и символов, а также влияет на сортировку. После создания базы данных изменить локаль нельзя.
9. Нажмите **Создать**.

MySQL semi-sync

Различия MySQL sync и MySQL semi-sync

В облачных базах данных доступны СУБД MySQL sync и MySQL semi-sync. Различия между ними — в таблице.

	MySQL sync	**MySQL semi-sync**
Репликация	Multi-master (синхронная) — для подтверждения записи нужно, чтобы все реплики получили данные	Master-replica (полусинхронная) — для подтверждения записи нужно, чтобы хотя бы одна из реплик получила данные
Отказоустойчивость	Можно создать кластер без реплик или только с двумя репликами	Можно создать кластер без реплик, с одной или с двумя репликами
Ограничения	На отказоустойчивые кластеры с репликами действуют ограничения	Нет ограничений
Подключение к кластеру	Для подключения к ProxySQL используется порт 6033	Для подключения к кластеру используется порт 3306

Версии и конфигурации MySQL semi-sync

Версии

Поддерживается версия MySQL semi-sync 8.

Конфигурации нод

При создании кластера облачных баз данных MySQL semi-sync можно выбрать для нод количество vCPU, RAM и размер локального диска.

Доступно два типа конфигураций:

- фиксированные конфигурации — несколько линеек с разными техническими характеристиками, в которых зафиксировано соотношение ресурсов;
- произвольные конфигурации — можно указать любое соотношение ресурсов.

Используемые процессоры зависят от выбранной конфигурации.

Около 5 ГБ локального диска во всех конфигурациях зарезервировано под операционную систему, компоненты сервиса и хранение логов. Остальной объем доступен для размещения баз данных.

После создания кластера можно изменить конфигурацию нод.

Процессоры

В линейках фиксированных конфигураций и произвольных конфигураций различаются доступные процессоры. Частота процессора влияет на скорость обработки запросов пользователей, выполнения сложных алгоритмов и операций с данными.

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

	Фиксированные конфигурации Standard, CPU, Memory	**Фиксированные конфигурации HighFreq**	**Фиксированные конфигурации Dedicated**	**Произвольные конфигурации**
Процессор	Intel® Xeon® Scalable, AMD EPYC™	Intel® Xeon® Gold 6354	Intel® Xeon® Gold 6240	Intel® Xeon® Scalable, AMD EPYC™
Частота процессора	2,2—2,4 ГГц	3,00 ГГц \Режим Turbo Boost 3,60 ГГц*	2,6 ГГц \Режим Turbo Boost 3,9 ГГц*	2,2—2,4 ГГц

* При нагрузке облачного сервера в 100% процессор работает с технологией Turbo Boost и максимальной частотой 3,6 ГГц для линейки HighFreq и 3,9 ГГц для линейки Dedicated. Так как процессор эмулируется, при тестировании будет отображаться частота 3,00 ГГц для линейки HighFreq и 2,6 ГГц для линейки Dedicated.

Фиксированные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

Фиксированную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Standard

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM, подходит для большинства СУБД. Рекомендуем использовать эту линейку, если вы не знаете профиль нагрузки.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
4	16 ГБ	128 ГБ
6	32 ГБ	256 ГБ
8	64 ГБ	512 ГБ
10	96 ГБ	768 ГБ
12	128 ГБ	1 ТБ
16	160 ГБ	1,5 ТБ
20	208 ГБ	2 ТБ

CPU

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к вычислениям. Например, если в базе данных выполняются аналитические запросы, множественные вложенные запросы или шифрование данных. Один из способов определить такой профиль нагрузки — отслеживать метрику `Load Average`, которая показывает среднее значение загрузки системы за одну, пять или 15 минут.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
6	16 ГБ	128 ГБ
8	32 ГБ	256 ГБ
10	64 ГБ	512 ГБ
12	96 ГБ	768 ГБ

16	128 ГБ	1 ТБ
20	160 ГБ	1,5 ТБ
24	208 ГБ	2 ТБ

Memory

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к кэшированию. Например, если в базе данных выполняются множественные, редкоповторяющиеся запросы к различным частям таблиц. Один из способов определить такой профиль нагрузки — отслеживать метрику `Попадание в кэш (Cash_hit_ratio)`, которая показывает процент данных в запросе, которые прочитаны из кэша.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	**RAM**	**Диск**
2	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ
10	128 ГБ	1 ТБ
14	160 ГБ	1,5 ТБ
16	208 ГБ	2 ТБ

HighFreq

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM.

Используется высокопроизводительное оборудование Enterprise-уровня:

- процессоры Intel® Xeon® Gold 6354 с частотой в режиме Turbo Boost до 3,6 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM ECC Reg 3,2 ГГц;
- SSD NVMe-диски повышенной производительности.

Количество vCPU	RAM	Диск
4	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	32 ГБ	256 ГБ
8	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	64 ГБ	512 ГБ
10	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ
10	96 ГБ	768 ГБ
12	96 ГБ	768 ГБ
10	120 ГБ	962 ГБ
12	120 ГБ	962 ГБ
14	120 ГБ	962 ГБ
12	152 ГБ	1,22 ТБ
14	152 ГБ	1,22 ТБ
16	184 ГБ	1,5 ТБ

Dedicated

Линейка фиксированных конфигураций с нодами кластера на отдельных облачных серверах. Каждый облачный сервер занимает весь выделенный хост (физический сервер). Подходит для пользователей, которым необходима физическая изоляция баз данных от других клиентов, максимальная производительность и максимальные размеры доступных ресурсов.

Используется высокопроизводительное оборудование Enterprise-уровня:

- один процессор Intel® Xeon® Gold 6240 с частотой в режиме Turbo Boost до 3,9 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM 64 ГБ DDR4 ECC Reg;

- два SSD NVMe-диска в RAID 1;
- две сетевые карты 2 × 25 GE для основной сети + MC-LAG со скоростью подключения 25 Гбит/с для сервисной сети (для резервного копирования, мониторинга, репликации данных в кластере).

	Количество vCPU	**RAM**	**Диск**
Medium	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 5 x 64 ГБ Физически на сервере 6 x 64 ГБ**	Доступно для СУБД 3,4 ТБ Физически на сервере 2 x 4 ТБ***
Large	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 7 x 64 ГБ Физически на сервере 8 x 64 ГБ**	Доступно для СУБД 7,2 ТБ Физически на сервере 2 x 8 ТБ***

* Чтобы повысить производительность кластера СУБД, используется технология гиперпоточности (Hyper-Threading Technology). Эта технология позволяет использовать 34 vCPU на базе физических 18 CPU. Такая производительность подойдет для высоконагруженных систем или аналитического профиля нагрузки.

** Одна планка оперативной памяти зарезервирована для сервисных служб, которые обслуживают физический сервер.

*** Чтобы обеспечить дополнительную отказоустойчивость, диски размещены в RAID 1. Это массив дисков с зеркалированием, поэтому для базы данных доступно 50% дискового пространства. Часть дискового пространства также зарезервировано для сервисных служб, которые обслуживают физический сервер.

Произвольные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

В произвольных конфигурациях используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Произвольную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Значения произвольных конфигураций

В произвольных конфигурациях можно выбрать соотношение ресурсов. При выборе конфигурации учтите:

- соотношение vCPU:RAM должно быть не менее, чем 1:4. Например, для 4 vCPU нужно не менее 16 ГБ RAM;
- соотношение vCPU:Локальный диск должно быть не менее, чем 1:32. Например, для 4 vCPU нужен диск размером не менее 128 ГБ.

Доступные значения зависят от пула.

	В пулах ru-1, ru-2, gis-1, uz-1, kz-1, ke-1	**В пулах ru-3, ru-9, ru-7, ru-8**
Количество vCPU	1—8	1—32
RAM	4—64 ГБ	4—256 ГБ
Размер локального диска	32—512 ГБ	32 ГБ — 1,23 ТБ

Создать кластер MySQL semi-sync

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Нажмите **Создать кластер**.
3. Введите имя кластера.
4. Выберите регион.
5. Выберите пул.
6. Выберите версию MySQL semi-sync. После создания версию будет нельзя изменить.
7. Выберите конфигурацию нод:
    - фиксированная — конфигурации с разным соотношением vCPU, RAM и локального диска;
    - произвольная — свободный выбор соотношения ресурсов.
8. Для фиксированной конфигурации выберите линейку конфигурации:
    - Standard;
    - CPU;
    - Memory;
    - HighFreq;
    - Dedicated.
9. Опционально: отметьте чекбокс **Добавить реплики** и укажите количество реплик. Реплики повышают отказоустойчивость кластера.
10. Выберите тип подсети, к которой будет подключен кластер:
    - приватная подсеть — подсеть без доступа из интернета. Можно подключить статический публичный IP-адрес;

    - публичная подсеть — все адреса публичной подсети доступны из интернета.
11. Выберите или создайте подсеть.
    Адреса присваиваются каждой ноде в кластере. Убедитесь, что количество адресов в подсети не меньше количества нод в кластере. Если после создания кластера вы планируете увеличить количество реплик, то выберите подсеть, в которой есть запас свободных адресов. После создания кластера подсеть нельзя изменить.
    Вы можете ограничить список адресов, с которых будет разрешен доступ в кластер баз данных.
12. Опционально: в приватной подсети вы можете подключить публичный IP-адрес к ноде кластера:
    - если вы выбрали существующую приватную подсеть — отметьте чекбокс **Публичный доступ к нодам кластера**, а затем чекбокс той ноды, к которой нужно предоставить публичный доступ. Приватная подсеть должна соответствовать требованиям;
    - если вы создаете новую приватную подсеть — подключите публичный IP-адрес после создания кластера.
13. Опционально: измените настройки СУБД, для этого нажмите **Изменить**. Мы рекомендуем менять значения настроек только при необходимости — неправильно подобранные значения могут снизить производительность кластера.
14. Нажмите **Создать кластер баз данных**. Кластер будет готов к работе, когда перейдет в статус `ACTIVE`.

Создать базу данных

После создания базы данных вы можете выдать пользователям доступ к ней.

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Откройте страницу кластера → вкладка **Базы данных**.
3. Нажмите **Создать базу данных**.
4. Введите имя базы данных.
5. Нажмите **Создать**.

MySQL sync

Различия MySQL sync и MySQL semi-sync

В облачных базах данных доступны СУБД MySQL sync и MySQL semi-sync. Различия между ними — в таблице.

	MySQL sync	**MySQL semi-sync**
Репликация	Multi-master (синхронная) — для подтверждения записи нужно, чтобы все реплики получили данные	Master-replica (полусинхронная) — для подтверждения записи нужно, чтобы хотя бы одна из реплик получила данные
Отказоустойчивость	Можно создать кластер без реплик или только с двумя репликами	Можно создать кластер без реплик, с одной или с двумя репликами
Ограничения	На отказоустойчивые кластеры с репликами действуют ограничения	Нет ограничений
Подключение к кластеру	Для подключения к ProxySQL используется порт 6033	Для подключения к кластеру используется порт 3306

Версии и конфигурации MySQL sync

Версии

Поддерживается версия MySQL sync 8.

Конфигурации нод

При создании кластера облачных баз данных MySQL sync можно выбрать для нод количество vCPU, RAM и размер локального диска.

Доступно два типа конфигураций:

- фиксированные конфигурации — несколько линеек с разными техническими характеристиками, в которых зафиксировано соотношение ресурсов;
- произвольные конфигурации — можно указать любое соотношение ресурсов.

Используемые процессоры зависят от выбранной конфигурации.

Около 5 ГБ локального диска во всех конфигурациях зарезервировано под операционную систему, компоненты сервиса и хранение логов. Остальной объем доступен для размещения баз данных.

После создания кластера можно изменить конфигурацию нод.

Процессоры

В линейках фиксированных конфигураций и произвольных конфигураций различаются доступные процессоры. Частота процессора влияет на скорость обработки запросов пользователей, выполнения сложных алгоритмов и операций с данными.

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

	Фиксированные конфигурации Standard, CPU, Memory	**Фиксированные конфигурации HighFreq**	**Фиксированные конфигурации Dedicated**	**Произвольные конфигурации**
Процессор	Intel® Xeon® Scalable, AMD EPYC™	Intel® Xeon® Gold 6354	Intel® Xeon® Gold 6240	Intel® Xeon® Scalable, AMD EPYC™
Частота процессора	2,2—2,4 ГГц	3,00 ГГц \Режим Turbo Boost 3,60 ГГц*	2,6 ГГц \Режим Turbo Boost 3,9 ГГц*	2,2—2,4 ГГц

* При нагрузке облачного сервера в 100% процессор работает с технологией Turbo Boost и максимальной частотой 3,6 ГГц для линейки HighFreq и 3,9 ГГц для линейки Dedicated. Так как процессор эмулируется, при тестировании будет отображаться частота 3,00 ГГц для линейки HighFreq и 2,6 ГГц для линейки Dedicated.

Фиксированные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

Фиксированную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Standard

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM, подходит для большинства СУБД. Рекомендуем использовать эту линейку, если вы не знаете профиль нагрузки.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
4	16 ГБ	128 ГБ
6	32 ГБ	256 ГБ
8	64 ГБ	512 ГБ
10	96 ГБ	768 ГБ
12	128 ГБ	1 ТБ
16	160 ГБ	1,5 ТБ
20	208 ГБ	2 ТБ

CPU

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к вычислениям. Например, если в базе данных выполняются аналитические запросы, множественные вложенные запросы или шифрование данных. Один из способов определить такой профиль нагрузки — отслеживать метрику `Load Average`, которая показывает среднее значение загрузки системы за одну, пять или 15 минут.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
6	16 ГБ	128 ГБ
8	32 ГБ	256 ГБ
10	64 ГБ	512 ГБ
12	96 ГБ	768 ГБ

16	128 ГБ	1 ТБ
20	160 ГБ	1,5 ТБ
24	208 ГБ	2 ТБ

Memory

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к кэшированию. Например, если в базе данных выполняются множественные, редкоповторяющиеся запросы к различным частям таблиц. Один из способов определить такой профиль нагрузки — отслеживать метрику `Попадание в кэш (Cash_hit_ratio)`, которая показывает процент данных в запросе, которые прочитаны из кэша.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	**RAM**	**Диск**
2	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ
10	128 ГБ	1 ТБ
14	160 ГБ	1,5 ТБ
16	208 ГБ	2 ТБ

HighFreq

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM.

Используется высокопроизводительное оборудование Enterprise-уровня:

- процессоры Intel® Xeon® Gold 6354 с частотой в режиме Turbo Boost до 3,6 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM ECC Reg 3,2 ГГц;
- SSD NVMe-диски повышенной производительности.

Количество vCPU	RAM	Диск
4	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	32 ГБ	256 ГБ
8	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	64 ГБ	512 ГБ
10	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ
10	96 ГБ	768 ГБ
12	96 ГБ	768 ГБ
10	120 ГБ	962 ГБ
12	120 ГБ	962 ГБ
14	120 ГБ	962 ГБ
12	152 ГБ	1,22 ТБ
14	152 ГБ	1,22 ТБ
16	184 ГБ	1,5 ТБ

Dedicated

Линейка фиксированных конфигураций с нодами кластера на отдельных облачных серверах. Каждый облачный сервер занимает весь выделенный хост (физический сервер). Подходит для пользователей, которым необходима физическая изоляция баз данных от других клиентов, максимальная производительность и максимальные размеры доступных ресурсов.

Используется высокопроизводительное оборудование Enterprise-уровня:

- один процессор Intel® Xeon® Gold 6240 с частотой в режиме Turbo Boost до 3,9 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM 64 ГБ DDR4 ECC Reg;

- два SSD NVMe-диска в RAID 1;
- две сетевые карты 2 × 25 GE для основной сети + MC-LAG со скоростью подключения 25 Гбит/с для сервисной сети (для резервного копирования, мониторинга, репликации данных в кластере).

	Количество vCPU	**RAM**	**Диск**
Medium	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 5 x 64 ГБ Физически на сервере 6 x 64 ГБ**	Доступно для СУБД 3,4 ТБ Физически на сервере 2 x 4 ТБ***
Large	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 7 x 64 ГБ Физически на сервере 8 x 64 ГБ**	Доступно для СУБД 7,2 ТБ Физически на сервере 2 x 8 ТБ***

* Чтобы повысить производительность кластера СУБД, используется технология гиперпоточности (Hyper-Threading Technology). Эта технология позволяет использовать 34 vCPU на базе физических 18 CPU. Такая производительность подойдет для высоконагруженных систем или аналитического профиля нагрузки.

** Одна планка оперативной памяти зарезервирована для сервисных служб, которые обслуживают физический сервер.

*** Чтобы обеспечить дополнительную отказоустойчивость, диски размещены в RAID 1. Это массив дисков с зеркалированием, поэтому для базы данных доступно 50% дискового пространства. Часть дискового пространства также зарезервировано для сервисных служб, которые обслуживают физический сервер.

Произвольные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

В произвольных конфигурациях используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Произвольную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Значения произвольных конфигураций

В произвольных конфигурациях можно выбрать соотношение ресурсов. При выборе конфигурации учтите:

- соотношение vCPU:RAM должно быть не менее, чем 1:4. Например, для 4 vCPU нужно не менее 16 ГБ RAM;
- соотношение vCPU:Локальный диск должно быть не менее, чем 1:32. Например, для 4 vCPU нужен диск размером не менее 128 ГБ.

Доступные значения зависят от пула.

	В пулах ru-1, ru-2, gis-1, uz-1, kz-1, ke-1	**В пулах ru-3, ru-9, ru-7, ru-8**
Количество vCPU	1—8	1—32
RAM	4—64 ГБ	4—256 ГБ
Размер локального диска	32—512 ГБ	32 ГБ — 1,23 ТБ

Создать кластер MySQL sync

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Нажмите **Создать кластер**.
3. Введите имя кластера.
4. Выберите регион.
5. Выберите пул.
6. Выберите версию MySQL sync. После создания версию будет нельзя изменить.
7. Выберите конфигурацию нод:
    - фиксированная — конфигурации с разным соотношением vCPU, RAM и локального диска;
    - произвольная — свободный выбор соотношения ресурсов.
8. Для фиксированной конфигурации выберите линейку конфигурации:
    - Standard;
    - CPU;
    - Memory;
    - HighFreq;
    - Dedicated.
9. Опционально: отметьте чекбокс **Добавить реплики** и укажите количество реплик. Реплики повышают отказоустойчивость кластера.
10. Выберите тип подсети, к которой будет подключен кластер:
    - приватная подсеть — подсеть без доступа из интернета. Можно подключить статический публичный IP-адрес;
    - публичная подсеть — все адреса публичной подсети доступны из интернета.

11. Выберите или создайте подсеть.
    Адреса присваиваются каждой ноде в кластере. Убедитесь, что количество адресов в подсети не меньше количества нод в кластере. Если после создания кластера вы планируете увеличить количество реплик, то выберите подсеть, в которой есть запас свободных адресов. После создания кластера подсеть нельзя изменить.
    Вы можете ограничить список адресов, с которых будет разрешен доступ в кластер баз данных.
12. Опционально: в приватной подсети вы можете подключить публичный IP-адрес к ноде кластера:
    - если вы выбрали существующую приватную подсеть — отметьте чекбокс **Публичный доступ к нодам кластера**, а затем чекбокс той ноды, к которой нужно предоставить публичный доступ. Приватная подсеть должна соответствовать требованиям;
    - если вы создаете новую приватную подсеть — подключите публичный IP-адрес после создания кластера.
13. Опционально: измените настройки СУБД, для этого нажмите **Изменить**. Мы рекомендуем менять значения настроек только при необходимости — неправильно подобранные значения могут снизить производительность кластера.
14. Нажмите **Создать кластер баз данных**. Кластер будет готов к работе, когда перейдет в статус `ACTIVE`.

Создать базу данных

После создания базы данных вы можете выдать пользователям доступ к ней.

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Откройте страницу кластера → вкладка **Базы данных**.
3. Нажмите **Создать базу данных**.
4. Введите имя базы данных.
5. Нажмите **Создать**.

Redis

Версии и конфигурации Redis

Версии

Поддерживается версия Redis 6.

Конфигурации нод

При создании кластера облачных баз данных Redis можно выбрать для нод необходимое количество vCPU, RAM и размер локального диска.

Доступны только фиксированные конфигурации.

Используемые процессоры зависят от выбранной линейки фиксированной конфигурации.

Около 5 ГБ локального диска во всех конфигурациях зарезервировано под операционную систему, компоненты сервиса и хранение логов. Остальной объем доступен для размещения баз данных.

После создания кластера можно изменить конфигурацию нод.

Процессоры

В линейках фиксированных конфигураций и произвольных конфигураций различаются доступные процессоры. Частота процессора влияет на скорость обработки запросов пользователей, выполнения сложных алгоритмов и операций с данными.

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

	Standard	**HighFreq**	**Dedicated**
Процессор	Intel® Xeon® Scalable, AMD EPYC™	Intel® Xeon® Gold 6354	Intel® Xeon® Gold 6240
Частота процессора	2,2—2,4 ГГц	3,00 ГГц \Режим Turbo Boost 3,6 ГГц*	2,6 ГГц \Режим Turbo Boost 3,9 ГГц*

* При нагрузке облачного сервера в 100% процессор работает с технологией Turbo Boost и максимальной частотой 3,6 ГГц для линейки HighFreq и 3,9 ГГц для линейки Dedicated. Так как процессор эмулируется, при тестировании будет отображаться частота 3,00 ГГц для линейки HighFreq и 2,6 ГГц для линейки Dedicated.

Фиксированные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

Фиксированную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Standard

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM, подходит для большинства СУБД. Рекомендуем использовать эту линейку, если вы не знаете профиль нагрузки.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
2	4 ГБ	30 ГБ
2	6 ГБ	50 ГБ
2	8 ГБ	60 ГБ
2	12 ГБ	90 ГБ
2	16 ГБ	120 ГБ
4	20 ГБ	150 ГБ
4	24 ГБ	180 ГБ
4	28 ГБ	200 ГБ
4	32 ГБ	250 ГБ
4	64 ГБ	500 ГБ
6	98 ГБ	700 ГБ

HighFreq

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM.

Используется высокопроизводительное оборудование Enterprise-уровня:

- процессоры Intel® Xeon® Gold 6354 с частотой в режиме Turbo Boost до 3,6 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM ECC Reg 3,2 ГГц;
- SSD NVMe-диски повышенной производительности.

Количество vCPU	RAM	Диск
2	4 ГБ	30 ГБ
2	6 ГБ	50 ГБ
2	8 ГБ	60 ГБ
2	12 ГБ	90 ГБ
2	16 ГБ	120 ГБ
4	20 ГБ	150 ГБ
4	24 ГБ	180 ГБ
4	28 ГБ	200 ГБ
4	32 ГБ	250 ГБ
4	64 ГБ	500 ГБ
6	98 ГБ	700 ГБ

Dedicated

Линейка фиксированных конфигураций с нодами кластера на отдельных облачных серверах. Каждый облачный сервер занимает весь выделенный хост (физический сервер). Подходит для пользователей, которым необходима физическая изоляция баз данных от других клиентов, максимальная производительность и максимальные размеры доступных ресурсов.

Используется высокопроизводительное оборудование Enterprise-уровня:

- один процессор Intel® Xeon® Gold 6240 с частотой в режиме Turbo Boost до 3,9 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM 64 ГБ DDR4 ECC Reg;
- два SSD NVMe-диска в RAID 1;
- две сетевые карты 2 × 25 GE для основной сети + MC-LAG со скоростью подключения 25 Гбит/с для сервисной сети (для резервного копирования, мониторинга, репликации данных в кластере).

	Количество vCPU	RAM	Диск
Medium	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 5 x 64 ГБ Физически на сервере 6 x 64 ГБ**	Доступно для СУБД 3,4 ТБ Физически на сервере 2 x 4 ТБ***
Large	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 7 x 64 ГБ Физически на сервере 8 x 64 ГБ**	Доступно для СУБД 7,2 ТБ Физически на сервере 2 x 8 ТБ***

* Чтобы повысить производительность кластера СУБД, используется технология гиперпоточности (Hyper-Threading Technology). Эта технология позволяет использовать 34 vCPU на базе физических 18 CPU. Такая производительность подойдет для высоконагруженных систем или аналитического профиля нагрузки.

** Одна планка оперативной памяти зарезервирована для сервисных служб, которые обслуживают физический сервер.

*** Чтобы обеспечить дополнительную отказоустойчивость, диски размещены в RAID 1. В RAID 1 используется зеркалирование, поэтому для базы данных доступно 50% дискового пространства. Часть дискового пространства также зарезервировано для сервисных служб, которые обслуживают физический сервер.

Создать кластер Redis

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Нажмите **Создать кластер**.
3. Введите имя кластера.
4. Выберите регион.
5. Выберите пул.
6. Выберите версию Redis. После создания версию будет нельзя изменить.
7. Выберите линейку конфигурации:
    - Standard;

    - HighFreq;
    - Dedicated.
8. Опционально: укажите количество реплик. Реплики повышают отказоустойчивость кластера.

9. Выберите политику вытеснения.

10. Введите пароль пользователя или нажмите **Сгенерировать**. Пароль должен содержать:

    - от 32 до 64 знаков;
    - латинские буквы разных регистров;
    - цифры;
    - специальные символы.
11. Скопируйте и сохраните пароль пользователя — он нужен для подключения к кластеру. Пароль нельзя будет посмотреть в панели управления, но можно изменить.

12. Выберите тип подсети, к которой будет подключен кластер:

    - приватная подсеть — подсеть без доступа из интернета. Можно подключить статический публичный IP-адрес;
    - публичная подсеть — все адреса публичной подсети доступны из интернета.
13. Выберите или создайте подсеть.

    Адреса присваиваются каждой ноде в кластере. Убедитесь, что количество адресов в подсети не меньше количества нод в кластере. Если после создания кластера вы планируете увеличить количество реплик, то выберите подсеть, в которой есть запас свободных адресов. После создания кластера подсеть нельзя изменить.

    Вы можете ограничить список адресов, с которых будет разрешен доступ в кластер баз данных.

14. Опционально: в приватной подсети вы можете подключить публичный IP-адрес к ноде кластера:

    - если вы выбрали существующую приватную подсеть — отметьте чекбокс **Публичный доступ к нодам кластера**, а затем чекбокс той ноды, к которой нужно предоставить публичный доступ. Приватная подсеть должна соответствовать требованиям;
    - если вы создаете новую приватную подсеть — подключите публичный IP-адрес после создания кластера.
15. Нажмите **Создать кластер баз данных**. Кластер будет готов к работе, когда перейдет в статус `ACTIVE`.

Kafka

Версии и конфигурации

Версии

Поддерживается версия Kafka 3.5.

Конфигурации нод

При создании кластера облачных баз данных Kafka можно выбрать для нод количество vCPU, RAM и размер локального диска.

Доступно два типа конфигураций:

- фиксированные конфигурации — несколько линеек с разными техническими характеристиками, в которых зафиксировано соотношение ресурсов;
- произвольные конфигурации — можно указать любое соотношение ресурсов.

Используемые процессоры зависят от выбранной конфигурации.

Около 5 ГБ локального диска во всех конфигурациях зарезервировано под операционную систему, компоненты сервиса и хранение логов. Остальной объем доступен для размещения баз данных.

После создания кластера можно изменить конфигурацию нод.

Процессоры

В линейках фиксированных конфигураций и произвольных конфигураций различаются доступные процессоры. Частота процессора влияет на скорость обработки запросов пользователей, выполнения сложных алгоритмов и операций с данными.

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

	Фиксированные конфигурации Standard, CPU, Memory	**Фиксированные конфигурации HighFreq**	**Фиксированные конфигурации Dedicated**	**Произвольные конфигурации**
Процессор	Intel® Xeon® Scalable, AMD EPYC™	Intel® Xeon® Gold 6354	Intel® Xeon® Gold 6240	Intel® Xeon® Scalable, AMD EPYC™

Частота процессора	2,2—2,4 ГГц	3,00 ГГц \Режим Turbo Boost 3,60 ГГц*	2,6 ГГц \Режим Turbo Boost 3,9 ГГц*	2,2—2,4 ГГц

* При нагрузке облачного сервера в 100% процессор работает с технологией Turbo Boost и максимальной частотой 3,6 ГГц для линейки HighFreq и 3,9 ГГц для линейки Dedicated. Так как процессор эмулируется, при тестировании будет отображаться частота 3,00 ГГц для линейки HighFreq и 2,6 ГГц для линейки Dedicated.

Фиксированные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

Фиксированную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Standard

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM, подходит для большинства СУБД. Рекомендуем использовать эту линейку, если вы не знаете профиль нагрузки.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
4	16 ГБ	128 ГБ
6	32 ГБ	256 ГБ
8	64 ГБ	512 ГБ
10	96 ГБ	768 ГБ
12	128 ГБ	1 ТБ
16	160 ГБ	1,5 ТБ
20	208 ГБ	2 ТБ

CPU

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к вычислениям. Например,

если в базе данных выполняются аналитические запросы, множественные вложенные запросы или шифрование данных. Один из способов определить такой профиль нагрузки — отслеживать метрику `Load Average`, которая показывает среднее значение загрузки системы за одну, пять или 15 минут.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
6	16 ГБ	128 ГБ
8	32 ГБ	256 ГБ
10	64 ГБ	512 ГБ
12	96 ГБ	768 ГБ
16	128 ГБ	1 ТБ
20	160 ГБ	1,5 ТБ
24	208 ГБ	2 ТБ

Memory

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM. Подходит для профилей нагрузки, которые требовательны к кэшированию. Например, если в базе данных выполняются множественные, редкоповторяющиеся запросы к различным частям таблиц. Один из способов определить такой профиль нагрузки — отслеживать метрику `Попадание в кэш (Cash_hit_ratio)`, которая показывает процент данных в запросе, которые прочитаны из кэша.

Используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Количество vCPU	RAM	Диск
2	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ

10	128 ГБ	1 ТБ
14	160 ГБ	1,5 ТБ
16	208 ГБ	2 ТБ
16	208 ГБ	2 ТБ
20	160 ГБ	1,5 ТБ

HighFreq

Линейка фиксированных конфигураций со сбалансированным соотношением vCPU:RAM.

Используется высокопроизводительное оборудование Enterprise-уровня:

- процессоры Intel® Xeon® Gold 6354 с частотой в режиме Turbo Boost до 3,6 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM ECC Reg 3,2 ГГц;
- SSD NVMe-диски повышенной производительности.

Количество vCPU	**RAM**	**Диск**
4	16 ГБ	128 ГБ
4	32 ГБ	256 ГБ
6	32 ГБ	256 ГБ
8	32 ГБ	256 ГБ
6	64 ГБ	512 ГБ
8	64 ГБ	512 ГБ
10	64 ГБ	512 ГБ
8	96 ГБ	768 ГБ
10	96 ГБ	768 ГБ
12	96 ГБ	768 ГБ
10	120 ГБ	962 ГБ
12	120 ГБ	962 ГБ

14	120 ГБ	962 ГБ
12	152 ГБ	1,22 ТБ
14	152 ГБ	1,22 ТБ
16	184 ГБ	1,5 ТБ

Dedicated

Линейка фиксированных конфигураций с нодами кластера на отдельных облачных серверах. Каждый облачный сервер занимает весь выделенный хост (физический сервер). Подходит для пользователей, которым необходима физическая изоляция баз данных от других клиентов, максимальная производительность и максимальные размеры доступных ресурсов.

Используется высокопроизводительное оборудование Enterprise-уровня:

- один процессор Intel® Xeon® Gold 6240 с частотой в режиме Turbo Boost до 3,9 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры;
- RAM 64 ГБ DDR4 ECC Reg;
- два SSD NVMe-диска в RAID 1;
- две сетевые карты 2 × 25 GE для основной сети + MC-LAG со скоростью подключения 25 Гбит/с для сервисной сети (для резервного копирования, мониторинга, репликации данных в кластере).

	Количество vCPU	**RAM**	**Диск**
Medium	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 5 x 64 ГБ Физически на сервере 6 x 64 ГБ**	Доступно для СУБД 3,4 ТБ Физически на сервере 2 x 4 ТБ***
Large	Доступно для СУБД 34 vCPU Физически на сервере 18 CPU*	Доступно для СУБД 7 x 64 ГБ Физически на сервере 8 x 64 ГБ**	Доступно для СУБД 7,2 ТБ Физически на сервере 2 x 8 ТБ***

* Чтобы повысить производительность кластера СУБД, используется технология гиперпоточности (Hyper-Threading Technology). Эта технология позволяет использовать 34 vCPU на базе физических 18 CPU. Такая производительность подойдет для высоконагруженных систем или аналитического профиля нагрузки.

** Одна планка оперативной памяти зарезервирована для сервисных служб, которые обслуживают физический сервер.

*** Чтобы обеспечить дополнительную отказоустойчивость, диски размещены в RAID 1. В RAID 1 используется зеркалирование, поэтому для базы данных доступно 50% дискового пространства. Часть дискового пространства также зарезервировано для сервисных служб, которые обслуживают физический сервер.

Произвольные конфигурации

Посмотреть доступность конфигураций в регионах можно в матрице доступности Облачные базы данных.

В произвольных конфигурациях используются процессоры Intel® Xeon® Scalable или AMD EPYC™ с частотой 2,2—2,4 ГГц. Посмотреть частоту процессора в разных конфигурациях можно в таблице Процессоры.

Произвольную конфигурацию можно выбрать при создании или масштабировании кластера в панели управления и через Terraform.

Значения произвольных конфигураций

В произвольных конфигурациях можно выбрать соотношение ресурсов. При выборе конфигурации учтите:

- соотношение vCPU:RAM должно быть не менее, чем 1:4. Например, для 4 vCPU нужно не менее 16 ГБ RAM;
- соотношение vCPU:Локальный диск должно быть не менее, чем 1:32. Например, для 4 vCPU нужен диск размером не менее 128 ГБ.

Доступные значения зависят от пула.

	В пулах ru-1, ru-2, gis-1, uz-1, kz-1, ke-1	**В пулах ru-3, ru-9, ru-7, ru-8**
Количество vCPU	2—8	2—32
RAM	8—64 ГБ	8—256 ГБ
Размер локального диска	64—512 ГБ	64 ГБ — 1,23 ТБ

Создать кластер Kafka

1. В панели управления перейдите в раздел **Облачная платформа → Базы данных**.
2. Нажмите **Создать кластер**.
3. Введите имя кластера.
4. Выберите регион.
5. Выберите пул.
6. Выберите версию Kafka. После создания версию будет нельзя изменить.
7. Выберите конфигурацию нод:
    - фиксированная — конфигурации с разным соотношением vCPU, RAM и локального диска;
    - произвольная — свободный выбор соотношения ресурсов.
8. Для фиксированной конфигурации выберите линейку конфигурации:
    - Standard;
    - CPU;
    - Memory;
    - HighFreq;
    - Dedicated.
9. Выберите тип подсети, к которой будет подключен кластер:
    - приватная подсеть — подсеть без доступа из интернета;
    - публичная подсеть — все адреса публичной подсети доступны из интернета.
10. Публичный IP-адрес использовать нельзя.
11. Выберите или создайте подсеть.

    Адреса присваиваются каждой ноде в кластере. Убедитесь, что количество адресов в сети не меньше количества нод в кластере. После создания кластера сеть нельзя изменить.

    Вы можете ограничить список адресов, с которых будет разрешен доступ в кластер баз данных.
12. Если вы выбрали приватную подсеть, укажите CIDR подсети.
13. Если вы хотите использовать протокол DHCP для приватной подсети, включите тумблер **DHCP**. Подробнее о протоколе DHCP в статье блога Selectel Принципы работы протокола DHCP.

14. Если вы выбрали публичную сеть, укажите размер подсети.

15. Опционально: измените настройки СУБД, для этого нажмите **Изменить**. Мы рекомендуем менять значения настроек только при необходимости — неправильно подобранные значения могут снизить производительность кластера.

16. Нажмите **Создать кластер баз данных**. Кластер будет готов к работе, когда перейдет в статус `ACTIVE`.

Часто задаваемые вопросы

Что такое Облачные базы данных

Это сервис облачной платформы Selectel. Позволяет быстро разворачивать в облаке оказоустойчивые кластеры баз данных с возможностью PITR-восстановления данных.

Настройка, конфигурация, обслуживание инфраструктуры, обеспечение безопасности и отказоустойчивости, выполнение бэкапов и масштабирование выполняются на стороне Selectel.

Что такое кластер баз данных

Это один или несколько нод баз данных (серверов), между которыми настроена репликация.

Основной сервер кластера — мастер-нода. В кластер можно добавить реплики — точные копии мастера. Если мастер становится недоступен, то одна из реплик берет роль мастера на себя, а вместо нее создается новая реплика (при этом адрес мастер-ноды меняется). Такой кластер надежен и используется для поддержки работы приложений.

Как понять, что кластер создался и все работает

Кластер успешно создан и работает, если у самого кластера и всех нод статус `ACTIVE`.

Можно ли менять настройки кластера после его создания

После создания кластера можно изменить:

- имя кластера;
- количество реплик в кластере MySQL sync, MySQL semi-sync, PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB и Redis;
- конфигурацию серверов кластера MySQL sync, MySQL semi-sync, PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, Redis и Kafka — в зависимости от СУБД уменьшить или увеличить количество vCPU, RAM и объем диска;
- настройки СУБД PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync и Kafka.

Нельзя изменить подсеть, в которую подключен кластер.

Что может пойти не так в работе кластера

В отказоустойчивом кластере может стать недоступной одна из нод. Это значит, что нода в течение минуты не посылала информацию о том, что она находится в статусе `ACTIVE`. В таком случае мы удалим существующую ноду и заменим ее на другую.

Если кластер состоит только из мастер-ноды, и она стала недоступна, то кластер также временно становится недоступен — пока вместо неактивного мастера не будет создан новый. При этом базы данных не пропадают, а становятся недоступны на какое-то время. Вы можете обратиться в техническую поддержку для решения проблемы или восстановить кластер из резервной копии — PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync, Redis.

Какие есть ограничения

Можно создать в рамках одного проекта:

- 10000 баз данных внутри всех кластеров;
- 1000 пользователей баз данных.

Количество кластеров ограничено квотами на ресурсы кластера — DBaaS vCPU, RAM и локальный диск. Вы можете увеличить лимиты проекта и квоты.

Кластер можно создавать в приватных и публичных подсетях. Для нод в приватной подсети можно подключить публичные IP-адреса.

Сколько стоит использование услуги Облачные базы данных

Цены на ресурсы облачных баз данных можно посмотреть на selectel.ru.

Есть ли возможность тонкой настройки СУБД

Настройки баз данных по умолчанию подобраны и зависят от выбранной конфигурации нод кластера.

Вы можете самостоятельно настроить PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync и Kafka.

Что произойдет, если на диске ноды кластера закончится место

Если диск кластера будет заполнен на 80%, уведомление появится в панели управления и будет отправлено на электронную почту Владельца аккаунта и тех пользователей, которые подписаны на категорию уведомлений «Услуги и сервисы».

Если диск кластера будет заполнен на 95% и более, кластер перейдет в статус `DISK_FULL` и будет работать только на чтение. Чтобы кластер работал на чтение и запись, очистите диск или масштабируйте кластер PostgreSQL, PostgreSQL для 1С, PostgreSQL TimescaleDB, MySQL sync, MySQL semi-sync, Redis и Kafka и выберите конфигурацию с бóльшим размером диска.

Почему мы не предоставляем роль суперпользователя

Суперпользователь может полностью контролировать базу данных и сервер, например изменять конфигурации, управлять пользователями и выполнять критически важные

команды. Предоставление такой роли может привести к нарушению безопасности, утечке данных и сбоям в работе системы, поэтому в продукте Облачные базы данных мы не предоставляем роль суперпользователя. Если вам необходимо выполнить действия, которые может выполнить только суперпользователь, создайте тикет.

Менеджер секретов

Общая информация

Менеджер секретов — единый безопасный сервис для:

- хранения секретов — чувствительных данных, например логинов, паролей для доступа к приложениям и базам данных, SSH-ключей, ключей API и других конфиденциальных данных из сервисов Selectel или внешних сервисов;
- управления сертификатами: Let's Encrypt® и TLS-сертификатами, хранения приватных ключей.

С секретами и сертификатами можно работать в панели управления, через API Менеджера секретов или Terraform.

В продукте поддерживаются: типы и роли пользователей, проекты.

Секреты

Все чувствительные данные, которые вы добавили в менеджер секретов, хранятся в едином хранилище. Доступ к хранилищу есть только у авторизованных пользователей.

Секреты хранятся в зашифрованном виде (AES 256-GCM). При передаче извлеченных данных используется TLS-шифрование — это обеспечивает защиту от прослушиваний и модификации данных.

Чувствительные данные, которые добавлены в менеджер секретов, можно не хранить в исходном коде, а настроить к ним автоматический доступ из приложений.

Доступна история операций с секретами.

Сертификаты

В менеджере секретов можно хранить TLS-сертификаты, полученные в центрах сертификации, и самоподписанные сертификаты. Для доменов, которые добавлены в DNS-хостинг, можно выпустить сертификат Let's Encrypt® с автоматическим обновлением.

Доступны алгоритмы шифрования открытого ключа сертификата — RSA и ECDSA.

Можно скачать сертификат, цепочку промежуточных сертификатов, корневой сертификат и приватный ключ.

Пользовательские сертификаты можно использовать в облачном балансировщике нагрузки.

Доступна история операций с сертификатами.

Стоимость

Сервис предоставляется бесплатно.

Работа с сертификатами

Пользовательские сертификаты

В менеджер секретов можно загрузить пользовательский сертификат, который вы выпустили в сторонних центрах сертификации. Для этого нужны:

- основной сертификат для домена;
- приватный ключ;
- опционально: один или несколько промежуточных сертификатов. Промежуточные сертификаты связывают конечный TLS-сертификат с корневым центром сертификации, с его помощью браузер убеждается в подлинности выпущенного TLS-сертификата;
- опционально: корневой сертификат — часть ключа, которым центры сертификации подписывают TLS-сертификат. Может потребоваться при использовании самоподписанных сертификатов.

Добавить пользовательский сертификат

1. Пользовательский сертификат действует только в том проекте, в который он был добавлен. Убедитесь, что вы находитесь в нужном проекте. Для этого откройте меню проектов (название текущего проекта) и выберите проект.

2. В панели управления перейдите в раздел **Облачная платформа** → **Менеджер секретов**.

3. Нажмите **Добавить сертификат**.

4. Выберите **Пользовательский сертификат**.

5. Введите имя сертификата.

6. Вставьте основной сертификат для домена. Он должен начинаться с `-----BEGIN CERTIFICATE-----` и заканчиваться `-----END CERTIFICATE-----`.

7. Вставьте приватный ключ. Он должен начинаться с `-----BEGIN PRIVATE KEY-----` и заканчиваться `-----END PRIVATE KEY-----`.

8. Опционально: чтобы добавить промежуточный сертификат, отметьте чекбокс **Добавить промежуточный сертификат** и в поле **Промежуточный сертификат** вставьте сертификат. Он должен начинаться с `-----BEGIN CERTIFICATE-----` и заканчиваться `-----END CERTIFICATE-----`.

   Если нужно добавить несколько промежуточных сертификатов, убедитесь, что все сертификаты (основной сертификат для домена, промежуточные и корневой)

создают полную цепочку. Значение `Issuer` основного сертификата должно совпадать со значением `Subject` первого промежуточного сертификата, значение `Issuer` первого промежуточного сертификата — с `Subject` второго промежуточного и так далее.

Промежуточные сертификаты можно добавить в поле **Промежуточный сертификат** в любом порядке, важно использовать полную цепочку.

9. Опционально: чтобы добавить корневой сертификат, отметьте чекбокс **Добавить корневой сертификат** и в поле **Корневой сертификат** вставьте сертификат. Он должен начинаться с `-----BEGIN CERTIFICATE-----` и заканчиваться `-----END CERTIFICATE-----`.

10. Нажмите **Добавить**.

Обновить пользовательский сертификат

1. В панели управления перейдите в раздел **Облачная платформа** → **Менеджер секретов**.

2. Откройте вкладку **Сертификаты**.

3. В меню ⁞ сертификата выберите **Обновить**.

4. Вставьте основной сертификат для домена. Он должен начинаться с `-----BEGIN CERTIFICATE-----` и заканчиваться `-----END CERTIFICATE-----`.

5. Вставьте приватный ключ. Он должен начинаться с `-----BEGIN PRIVATE KEY-----` и заканчиваться `-----END PRIVATE KEY-----`.

6. Опционально: чтобы добавить промежуточный сертификат, отметьте чекбокс **Добавить промежуточный сертификат** и в поле **Промежуточный сертификат** вставьте сертификат. Он должен начинаться с `-----BEGIN CERTIFICATE-----` и заканчиваться `-----END CERTIFICATE-----`.

   Если нужно добавить несколько промежуточных сертификатов, убедитесь, что все сертификаты (основной сертификат для домена, промежуточные и корневой) создают полную цепочку. Значение `Issuer` основного сертификата должно совпадать со значением `Subject` первого промежуточного сертификата, значение `Issuer` первого промежуточного сертификата — с `Subject` второго промежуточного и так далее.

   Промежуточные сертификаты можно добавить в поле **Промежуточный сертификат** в любом порядке, важно использовать полную цепочку.

7. Опционально: чтобы добавить корневой сертификат, отметьте чекбокс **Добавить корневой сертификат** и в поле **Корневой сертификат** вставьте сертификат. Он должен начинаться с `-----BEGIN CERTIFICATE-----` и заканчиваться `-----END CERTIFICATE-----`.

8. Нажмите **Обновить**.

Сертификаты от Let’s Encrypt®

Если выпустить сертификат Let’s Encrypt® в менеджере секретов, проверка DNS-01 будет происходить автоматически. DNS-записи домена хранятся в инфраструктуре Selectel, поэтому сервис самостоятельно создает TXT-запись для выпуска сертификата. Сервис отследит дату окончания сертификата и автоматически обновит его за 30 дней до истечения срока действия. При самостоятельном выпуске сертификата нужно подтверждать право на домен и проходить проверку, а затем обновлять сертификат каждые 60 дней.
Сертификат действует только в том проекте, в котором он был выпущен.

Выпустить сертификат Let’s Encrypt®

Можно выпустить Let’s Encrypt® сертификат, который будет действовать:

- только для основного домена или для основного домена и всех его поддоменов (Wildcard-сертификат);
- только для поддомена. Сертификат не будет действовать для основного домена.

После выпуска сертификата Let’s Encrypt® сайт, сервис или приложение не будет автоматически открываться по протоколу HTTPS — нужно скачать сертификат и установить его на вашем веб-сервере.

1. Создайте зону для домена в DNS-хостинге.

2. Делегируйте домен.

3. В панели управления перейдите в раздел **Облачная платформа → Менеджер секретов**.

4. Откройте вкладку **Сертификаты**.

5. Нажмите **Добавить сертификат**.

6. Выберите **Сертификаты от Let’s Encrypt®**.

7. Введите имя сертификата.

8. Выберите домен, который вы делегировали в DNS-хостинг на шаге 2.

9. Опционально: чтобы добавить в сертификат для основного домена поддомен, нажмите **Добавить дополнительный домен**.

   Введите имя поддомена. Чтобы выпустить Wildcard-сертификат, введите поддомен вида `*.example.com`

10. Нажмите **Выпустить сертификат**.

Скачать сертификат Let's Encrypt®

1. В панели управления перейдите в раздел **Облачная платформа** → **Менеджер секретов**.
2. Откройте вкладку **Сертификаты** → страница сертификата.
3. В блоке **Файлы сертификата** выберите сертификат, цепочку промежуточных сертификатов, корневой сертификат и приватный ключ.
4. Нажмите **Скачать**.

Посмотреть статус сертификата Let's Encrypt®

1. В панели управления перейдите в раздел **Облачная платформа** → **Менеджер секретов**.

2. Откройте вкладку **Сертификаты**.

3. Посмотрите статус в строке сертификата → столбец **Статус**.

ACTIVE	Сертификат действителен и готов к использованию
CREATING	Происходит выпуск сертификата и сохранение секретов
RENEWING	До окончания срока действия сертификата осталось 30 дней, происходит автоматический перевыпуск
INVALID	Сертификат недействителен по одной из причин: • подписан неверно; • нарушена цепочка доверия сертификатов (не удалось проверить корневой сертификат или истек срок действия промежуточного сертификата); • невозможно проверить подпись сертификата; • не прошел DNS-01 проверку

ERROR	При выпуске сертификата произошла ошибка. Проверьте, что у регистратора вашего домена созданы NS-записи, указывающие на серверы Selectel: `a.ns.selectel.ru`, `b.ns.selectel.ru`, `c.ns.selectel.ru`, `d.ns.selectel.ru`. Если проблема осталась, создайте тикет

Посмотреть историю операций

В истории операций фиксируется дата, время, имя сертификата и пользователь, который совершил операцию с сертификатом. Возможные операции:

- `CREATE` — создание;
- `READ` — просмотр;
- `DELETE` — удаление.

1. В панели управления перейдите в раздел **Облачная платформа** → **Менеджер секретов**.
2. Откройте вкладку **История операций**.
3. Опционально: чтобы отфильтровать историю по сертификатам, отметьте чекбокс **Отображать историю операций для сертификатов**.

Удалить сертификат

1. В панели управления перейдите в раздел **Облачная платформа** → **Менеджер секретов**.
2. Откройте вкладку **Сертификаты**.
3. В меню ⋮ сертификата выберите **Удалить**.
4. Введите имя сертификата для подтверждения удаления.
5. Нажмите **Удалить**.

Работа с секретами

Добавить секрет

1. В панели управления перейдите в раздел **Облачная платформа** → **Менеджер секретов**.
2. Откройте вкладку **Секреты**.
3. Нажмите **Добавить секрет**.
4. Введите имя секрета — его уникальный ключ. После создания секрета имя нельзя будет изменить.
5. Введите значение секрета: пароль, ключ API, ключ сертификата или другое. Ограничение — 65536 символов.
6. Опционально: введите описание секрета.
7. Нажмите **Добавить**.

Посмотреть историю операций

В истории операций фиксируется дата, время, имя секрета и пользователь, который совершил операцию с секретом. Возможные операции:

- `CREATE` — создание;
- `READ` — просмотр;
- `UPDATE` — обновление;
- `DELETE` — удаление.

1. В панели управления перейдите в раздел **Облачная платформа** → **Менеджер секретов**.
2. Откройте вкладку **История операций**.
3. Опционально: чтобы отфильтровать историю по секретам, отметьте чекбокс **Отображать историю операций для секретов**.

Удалить секрет

1. В панели управления перейдите в раздел **Облачная платформа** → **Менеджер секретов**.
2. Откройте вкладку **Секреты**.
3. В строке с секретом нажмите 🗑️.
4. Введите имя секрета для подтверждения удаления.
5. Нажмите **Удалить**.

Объектное хранилище

Общая информация

Объектное хранилище — сервис Selectel для хранения и раздачи неограниченного объема неструктурированных и полуструктурированных данных.

Данные объектного хранилища хранятся в пуле ru-1.

Объектное хранилище регулируется условиями использования и по умолчанию соответствует 152-ФЗ.

В продукте поддерживаются типы и роли пользователей и проекты.

Как работать с объектным хранилищем

Работать с хранилищем можно:

- через S3 API, Swift API и Selectel Storage API. Для работы через API можно использовать различные инструменты (Rclone, AWS CLI, s3cmd и другие);
- по протоколу FTP. Он использует Swift API для трансляции запросов в объектное хранилище;
- через панель управления Selectel, которая выполняет запросы в объектное хранилище через Swift API и Selectel Storage API. У панели управления есть ограничения на работу с большим количеством объектов и с объектами большого размера;
- с помощью Terraform.

Решаемые задачи

Объектное хранилище является универсальным, его можно использовать для:

- раздача статической информации (данных сайтов и приложений), потоковая передача данных и т. д. Для ускорения раздачи данных можно подключить CDN;
- хранение резервных копий и архивов. Вы можете настроить резервное копирование сервера по расписанию, чтобы переносить важные данные в хранилище;
- хранение больших объемов данных для машинного обучения и аналитики;
- размещение статических сайтов.

Принцип работы

Объектное хранилище построено на базе программно-определяемой распределенной системы хранения данных. Данные в хранилище хранятся в виде объектов и реплицируются на три независимых сервера, которые находятся в разных стойках.

Объекты хранятся в контейнерах и наследуют их настройки.

Объектное хранилище имеет плоскую адресную структуру — в хранилище нет папок и иерархии, благодаря чему вы можете получать быстрый доступ к объектам по протоколу HTTP.

Каждый объект в хранилище содержит:

- данные;
- уникальный идентификатор, который используется хеш-функцией для определения местоположения объекта;
- метаданные. Вы можете добавлять свои метаданные, чтобы реализовать собственную систему хранения и обработки данных.

Модель оплаты и цены объектного хранилища

Баланс

Для оплаты ресурсов объектного хранилища в зависимости от типа баланса в аккаунте используется единый баланс или баланс хранилища и CDN. Деньги списываются с баланса каждый час в соответствии с моделью оплаты.

Оплатить ресурсы можно разными типами средств: основными средствами, бонусами или ВК бонусами.

Перед началом использования хранилища пополните баланс.

Модель оплаты

Объектное хранилище оплачивается по модели pay-as-you-go — оплата за потребленные ресурсы списывается каждый час.

Пока в хранилище есть загруженные объекты, оно тарифицируется — для прекращения оплаты удалите все данные.

Блокировка ресурсов, если на балансе недостаточно денег

Если на балансе недостаточно денег для оплаты потребленных ресурсов за предыдущий час, работа объектного хранилища приостанавливается:

- доступ к данным (чтение, изменение) блокируется;
- хранение данных продолжает тарифицироваться.

Данные будут храниться в течение 30 календарных дней. Если деньги не поступят, все данные будут удалены без возможности восстановления.

Чтобы на балансе всегда было достаточно денег, можно настроить уведомления о балансе и автопополнение баланса.

Цены

Цены на ресурсы можно посмотреть на selectel.ru.

Рассчитать примерную стоимость использования объектного хранилища можно в калькуляторе ресурсов.

На стоимость влияет класс хранения и потребление ресурсов:

- количество запросов к API;
- объем исходящего трафика (ГБ);
- объем хранения (МБ/час).

Классы хранения

Класс хранения влияет на цену каждого ресурса:

- холодное хранение — подходит для хранения редко используемых данных. Низкая цена на хранение, но дорогие запросы к API и исходящий трафик. Цены на ресурсы фиксированные для любого объема потребления;
- стандартное хранение — подходит для хранения и раздачи часто используемых данных. Высокая цена на хранение, но дешевые запросы к API и исходящий трафик. Цены на ресурсы зависят от объема потребления (кроме цен на запросы API).

Технически и по скорости классы одинаковые.

Количество запросов к API

Запросы к API отправляются при любых операциях с данными.

Тарифицируются запросы GET, HEAD, PUT, POST, COPY.

Не тарифицируются запросы DELETE и запросы, на которые был возвращен ответ HTTP с кодами 403, 500, 501, 502, 503, 504.

Объем исходящего трафика

Тарифицируется трафик из хранилища в интернет (просмотр и скачивание объектов).

Трафик внутри Selectel и входящий трафик не тарифицируются.

Объем хранения

Каждый час с баланса списываются деньги за текущий объем хранения. При использовании сегментированной загрузки тарифицируются сегменты объекта и файл манифеста. Посмотреть текущий объем данных в хранилище можно в панели управления под заголовком раздела **Объектное хранилище** → **Контейнеры**.

При подсчете потребления за сутки или месяц суммируется объем хранения, потребленный за каждый час (МБ/час). Если объем хранения был изменен, для стандартного хранилища оплата за часы после изменения будет соответствовать новому объему.

Пустые контейнеры также занимают место в хранилище (4 КБ) и тарифицируются.

Посмотреть потребление

Посмотреть потребление ресурсов можно в панели управления в разделе **Объектное хранилище** → **Расходы**. Если объекты хранилища раздаются через CDN, смотрите потребление в разделе **CDN** → **Расходы**.

Данные представлены в виде графиков потребления и оплаты. Вы можете посмотреть потребление на вкладке **Потреблено** по всем видам ресурсов и отсортировать графики по нужному временному интервалу.

Чтобы выгрузить детализацию потребления и оплаты в формате `.csv`, нажмите **Скачать CSV** и выберите, как будут сгруппированы строки в выгрузке (по часам, дням, неделям, месяцам, годам).

Отчетные документы

После списания денег за использование объектного хранилища можно получить отчетные документы.

Ограничения объектного хранилища

Мы рекомендуем загружать объекты размером более 100 МБ с помощью сегментированной загрузки через S3 API или Swift API.

Лимиты хранилища и лимиты контейнера вы устанавливаете самостоятельно.

Ограничения сущностей хранилища

Если превысить лимит, сервер вернет ответ с кодом `429 Too Many Requests` и сообщением `Rate Limit exceeded`.

- Контейнеры
- Объекты
- Заголовки

Максимальное количество контейнеров в проекте	2000*
Максимальное количество контейнеров с Virtual-Hosted адресацией в проекте	100 (в рамках 2000)

Максимальный размер имени контейнера	128 символов UTF-8
Максимальный размер политики доступа	20 КБ
Максимальное количество объектов в контейнере	Не ограничено

* В панели управления отображаются первые 1000 контейнеров. Если контейнеров больше, посмотреть полный список можно через API.

Ограничения запросов API

Ограничения на запросы в API распространяются на весь аккаунт.

Тип запросов	Лимит (запросов в секунду)	Сообщение от сервера
Все запросы	2000	Too many authorized requests
GET + HEAD	1000	Too many GET requests
POST	200	Too many POST requests
PUT	300	Too many PUT requests
DELETE	300	Too many DELETE requests

Работа с хранилищем

Управлять доступом в объектное хранилище

Доступ к ресурсам объектного хранилища регулируется:

- ролевой моделью — определяет доступ в рамках аккаунта и проекта;
- политикой доступа — определяет доступ в рамках контейнера.

При получении запроса на действие в объектном хранилище сначала проверяется доступ по ролевой модели. Если ролевая модель разрешает доступ, проверяется политика доступа, если нет — доступ запрещается.

Для доступа через API или по FTP выдайте ключи.

Доступ в рамках ролевой модели

Объектное хранилище поддерживает ролевую модель:

- Владелец аккаунта — имеет полный доступ ко всем проектам и управлению всеми ресурсами объектного хранилища и других продуктов в аккаунте через панель управления, а также управлению пользователями;
- Администратор аккаунта — имеет полный доступ ко всем проектам и управлению всеми ресурсами объектного хранилища, кроме пользователей;
- Администратор пользователей — может создавать пользователей и не имеет доступа к ресурсам объектного хранилища;
- Администратор проекта — имеет полный доступ к управлению объектным хранилищем и другими продуктами в проекте, кроме управления пользователями;
- Наблюдатель аккаунта — может просматривать ресурсы объектного хранилища и других продуктов во всех проектах;
- Наблюдатель проекта — может просматривать ресурсы объектного хранилища и других продуктов в своем проекте;
- Администратор объектного хранилища — имеет полный доступ к управлению объектным хранилищем в проекте без доступа к другим продуктам и управлению пользователями;
- Пользователь объектного хранилища — по умолчанию не имеет доступа к просмотру и управлению ресурсами объектного хранилища. Он получает доступ к управлению объектами тех контейнеров, для которых настроена политика доступа, если правила политики разрешают доступ этому пользователю. Пользователю недоступно подключение по FTP.
- Пользователи панели управления
- Сервисные пользователи

Доступ в рамках политики доступа

Если роль пользователя предусматривает доступ к объектному хранилищу, доступ к конкретному контейнеру зависит от наличия и настроек политики доступа:

- если политика доступа не создана, доступ будет разрешен всем пользователям с доступом в рамках ролевой модели, кроме роли Пользователь объектного хранилища;
- если политика доступа создана, запрещено все, что не разрешено правилами политики.

Подробнее о работе политики доступа в разделе Политика доступа.

Ключи для доступа через API

Выдавать ключи для доступа к хранилищу через API можно только сервисным пользователям.

В зависимости от типа API пользователю понадобится:

- токен Keystone, используется для доступа через Selectel Storage API и Swift API;
- S3-ключ (EC2-ключ), используется для подписи запросов S3 API и по FTP. Состоит из пары значений — Access Key ID и Secret Key.

Выдать S3-ключ

Выдавать S3-ключи (EC2-ключи) можно только сервисным пользователям с ролью с доступом в объектное хранилище.

Выдать S3-ключ сервисному пользователю может только Владелец аккаунта или Администратор пользователей. Получить S3-ключ самостоятельно сервисный пользователь не может.

Для каждого проекта необходимо создавать отдельный ключ. На один проект можно выпустить несколько ключей.

1. В панели управления перейдите в раздел **Управление доступом** → **Управление пользователями**.

2. Откройте вкладку **Сервисные пользователи**.

3. Откройте страницу сервисного пользователя.

4. В блоке **S3 ключи** нажмите **Добавить ключ**.

5. Введите имя ключа.

6. Выберите проект, для которого будет работать ключ.

7. Нажмите **Сгенерировать**. Будет сгенерировано два значения:

    - Access key — Access Key ID, идентификатор ключа;
    - Secret key — Secret Access Key, секретный ключ.

8. Нажмите **Скопировать** и сохраните ключ — после закрытия окна его нельзя будет просмотреть.

Лимиты объектного хранилища

По умолчанию у объектного хранилища не установлены лимиты, вы можете хранить любой объем файлов до тех пор, пока на балансе есть деньги для оплаты хранилища.

Чтобы контролировать объем загружаемых данных и потребление ресурсов, вы можете установить лимит на объем данных, которые хранятся во всех контейнерах проекта. Лимиты на определенный контейнер можно установить отдельно, подробнее в инструкции Лимиты контейнера.

Если лимит установлен:

- когда в хранилище будет занято 90% места от установленного лимита, в панели управления появится предупреждение;
- когда лимит будет достигнут, в панели управления появится уведомление, а при попытке загрузки объектов хранилище вернет ошибку. Чтобы продолжить загрузку, освободите место или увеличьте лимит.

Установить лимит

1. В панели управления перейдите в раздел **Объектное хранилище** → **Настройки**.
2. В блоке **Лимиты** нажмите **Изменить лимит**.
3. Включите тумблер **Максимальный размер**.
4. Введите значение лимита в гигабайтах.
5. Нажмите **Сохранить**.

Кеширование

При первом запросе пользователем объекта в публичном контейнере объект сохраняется в кеше объектного хранилища. Если объект закеширован, при повторном запросе пользователь сразу получит его с кеш-сервера хранилища, а не с его бекенд-сервера.

Кеш очищается автоматически при изменении тела объекта, система кеширования отслеживает изменения по хешу MD5.

Вы можете изменить настройки кеширования для контейнера через заголовок `Cache-Control`.

Чтобы получить актуальную версию объекта, можно очистить кеш вручную — это обновит контент на кеш-сервере.

Очистить кеш

1. В панели управления перейдите в раздел **Объектное хранилище → Очистка кеша**.
2. Вставьте ссылки на каждый объект, кеш которого нужно очистить.
3. Нажмите **Очистить кеш**.

Настроить кеширование

1. В панели управления перейдите в раздел **Объектное хранилище → Контейнеры**.
2. Откройте страницу контейнера → вкладка **Конфигурация**.
3. В поле **Cache-Control** введите настройки кеширования через запятую — например, `public, no-cache, private, max-age=31536000`, где `31536000` — максимальное время хранения кеша в секундах.
4. Нажмите **Сохранить**.

Пример настройки резервного копирования по расписанию

Цель настройки

Создать скрипт, который будет регулярно запускать консольный клиент, архивировать и переносить важные данные в объектное хранилище.

Что нужно для настройки

- консольный клиент (в примере S3cmd с инструментом для автоматизации crontab);
- облачный или выделенный сервер с установленной Ubuntu версии не ниже 18.04;
- пользователь с доступом в объектное хранилище.

Результат настройки

Скрипт создаст резервную копию файла или каталога с помощью tar и загрузит резервную копию в объектное хранилище с помощью s3cmd.

Шаги настройки

1. Создайте скрипт.
2. Перенесите файлы в объектное хранилище.
3. Настроить управление потоком.
4. Проверьте скрипт.
5. Опционально: автоматизируйте резервное копирование через crontab или Cyberduck.

Работа с контейнерами

Создать контейнер

1. В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.

2. Нажмите **Создать контейнер**.

3. Введите имя контейнера. Для совместимости с S3 API имя контейнера должно быть уникально в рамках объектного хранилища и соответствовать правилам именования бакетов Amazon S3, подробнее в инструкции Bucket naming rules документации Amazon.

4. Выберите тип контейнера:

    - приватный — для хранения резервных копий и других данных с доступом по логину и паролю или авторизационному токену;
    - публичный — для раздачи контента сайта или веб-приложения, доступен без авторизации.
5. Выберите класс хранения:

    - стандартное хранение — для хранения и раздачи часто запрашиваемых данных;
    - холодное хранение — для хранения редко запрашиваемых данных.
6. Класс хранения влияет только на стоимость ресурсов, технически и по скорости классы одинаковые. После создания контейнера класс хранения изменить нельзя.

7. Если вам нужен контейнер с Virtual-Hosted адресацией для работы с S3 API, в блоке **Тип адресации** выберите **vHosted**. Включить Virtual-Hosted адресацию можно только один раз.

8. Нажмите **Создать контейнер**.

Политика доступа к контейнеру

Доступ к контейнеру можно задать через политику доступа (Bucket policy). Политика состоит из правил, которые разрешают или запрещают действия с ресурсом (контейнером или группой объектов) для всех или выбранных принципалов (пользователей). Основной принцип — если политика доступа создана, запрещено все, что не разрешено.

Политика доступа работает только с S3 API.

Политика доступа имеет ограничение на максимальный размер в 20 КБ.

Политика доступа может распространяться на любого пользователя, которому разрешен доступ к хранилищу в соответствии с ролевой моделью, а также определяет доступ для пользователей с ролью Пользователь объектного хранилища. Подробнее о

взаимодействии ролевой модели и политик доступа в инструкции Управлять доступом в объектном хранилище.

Управлять политиками доступа могут только пользователи с ролью Владелец аккаунта, Администратор аккаунта или Администратор проекта, в котором находится контейнер.

Создавать политики доступа и управлять ими можно в панели управления или через S3 API в соответствии с требованиями к структуре политики.

Правила

Правила бывают двух типов: разрешающие (`Allow`) и запрещающие (`Deny`).

Разрешение или запрет распространяется на действия, ресурсы и принципалов, добавленных в правило.

Если политика содержит несколько правил, они применяются следующим образом:

- если хотя бы одно разрешающее правило выполняется, доступ будет разрешен;
- если хотя бы одно запрещающее правило выполняется, доступ будет запрещен;
- если выполняются одновременно разрешающие и запрещающие правила, доступ будет запрещен;
- если ни одно правило не выполняется, доступ будет запрещен.

Принципалы

Правило применяется в отношении запросов от принципалов (пользователей):

- на авторизованные запросы определенных пользователей, указываются идентификаторы пользователей (посмотреть идентификатор сервисного пользователя можно в панели управления);
- на все авторизованных и неавторизованные запросы, обозначается символом `*`.

Добавлять в качестве принципалов пользователей панели управления в политики доступа можно только при настройке политики через панель управления.

Ресурсы

Ресурсы — контейнер или набор объектов, на которые будет распространяться правило. Указывать можно только ресурсы, связанные с контейнером, для которого настраивается политика.

Ресурсы можно указывать в форматах:

- `arn:aws:s3:::<container-name>` — ресурс контейнера, можно указать только один ресурс такого формата (контейнер, для которого настраивается политика). Ресурс будет работать для действий, связанных с настройкой контейнера, и не распространяется на его объекты;

- `arn:aws:s3:::<container-name>/<prefix>` — ресурс объектов контейнера, где `<prefix>` — префикс, на объекты с которым будет распространяться правило. Если указать `*`, в ресурсы будут включены все объекты контейнера;

- `arn:aws:s3:::<container-name>/${<variable-name>}` — ресурс объектов контейнера, где `<variable-name>` — имя подстановочной переменной (ключа), которая выполняет роль префикса.

Лимиты контейнера

По умолчанию на контейнеры не установлены лимиты, вы можете хранить любой объем файлов в контейнере до тех пор, пока на балансе есть деньги для оплаты хранилища.

Вы можете ограничить хранение объектов в контейнере с помощью лимитов:

- на суммарный размер объектов;
- количество объектов;
- время хранения объектов в контейнере.

При достижении лимита на суммарный размер файлов или количество файлов загрузить объекты в контейнер будет невозможно.

При установке лимита на время хранения файлов в контейнере он применяется только для новых объектов — в метаданных каждого объекта автоматически проставляется заголовок с датой, когда объект будет удален. При изменении или удалении лимита заголовок для ранее загруженных объектов не изменится — загруженные до установки лимита объекты не будут удалены, а объекты с заголовком в метаданных будут удалены в указанное время даже в случае сброса лимитов контейнера. Подробнее об отложенном удалении в документации Swift API.

Вы можете установить лимит хранения на все хранилище (все контейнеры в рамках проекта), подробнее в инструкции Лимиты объектного хранилища.

Разместить статический веб-сайт

Статические сайты состоят из набора файлов (HTML, JS, графики, шрифтов), которые можно хранить в виде объектов в контейнере. Сайт будет открываться по адресу публичного домена контейнера или пользовательского домена, если он добавлен к контейнеру.

Есть два способа размещения веб-сайта:

- хостинг — вы указываете главную страницу веб-сайта, которая хранится в виде объекта в публичном контейнере;
- веб-листинг — вместо отображения главной страницы вы включаете возвращение списка объектов в контейнере и задаете свои CSS-стили.

Настроить хостинг

1. В контейнер загрузите объект — HTML-файл, который будет главной страницей.
2. В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.
3. Откройте страницу контейнера → вкладка **Веб-сайт**.
4. В блоке **Веб-сайт** включите тумблер.
5. Откройте вкладку **Хостинг**.
6. Введите путь до объекта с главной страницей с расширением `.html`.
7. Нажмите **Сохранить**.

Настроить веб-листинг

1. Если вы хотите хранить файл с CSS-стилями в контейнере, загрузите его.

2. В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.

3. Откройте страницу контейнера → вкладка **Веб-сайт**.

4. В блоке **Веб-сайт** включите тумблер.от того, где хранится файл:

    - в контейнере — введите путь до объекта с CSS-стилями;
    - на стороннем ресурсе — введите URL-адрес файла с CSS-стилями.
5. Нажмите **Сохранить**.

Настроить страницу ошибки

Если пользователи будут обращаться к несуществующему объекту, возникнет ошибка, которую можно обрабатывать двумя способами:

- возвращать другой объект из контейнера;
- выполнять переадресацию запроса на внешний URL.

Возвращать объект из контейнера

1. В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.
2. Откройте страницу контейнера → вкладка **Веб-сайт**.
3. В блоке **Страница ошибки** включите тумблер.
4. Опционально: если вы хотите, чтобы объект возвращался с кодом 200, выберите его в качестве кода ответа. По умолчанию ответ на запрос будет с кодом 400.
5. В поле **Ресурс** введите путь до объекта со страницей ошибки с расширением `.html`.
6. Нажмите **Сохранить**.

Выполнять переадресацию запроса

1. В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.
2. Откройте страницу контейнера → вкладка **Веб-сайт**.

3. В блоке **Страница ошибки** включите тумблер.
4. Выберите код ответа 307.
5. В поле **Ресурс** введите валидный внешний URL, на который будет выполнена переадресация, если запрашиваемый объект отсутствует.
6. Нажмите **Сохранить**.

Пути до объектов

При размещении статического веб-сайта или настройке страницы ошибки потребуется ввести путь до объекта в контейнере — абсолютный или относительный.

Абсолютный путь

Абсолютный путь всегда начинается с символа `/` и указывается в формате `/<prefix>/<object_name>`, где:

- `<prefix>` — префикс (путь до объекта) — при наличии;
- `<object_name>` — имя объекта с расширением.

Если указан абсолютный путь, при запросе объекта логика хранилища будет всегда искать его относительно корня контейнера — по адресу `<uuid>.selstorage.ru/<container_name>`. Если в запросе после имени контейнера есть префикс, он будет проигнорирован.

Если указать некорректный путь, объект не будет возвращен.

Например, если полный адрес объекта `<uuid>.selstorage.ru/container/prefix/file.html`, в качестве пути вы указали `/prefix/file.html` и запрос выполняется по адресу `<uuid>.selstorage.ru/container/prefix/`, объект будет возвращен.

Относительный путь

Относительный путь никогда не начинается с символа `/` и указывается в формате `<prefix>/<object_name>` или `<object_name>`, где:

- `<prefix>/` — опционально: префикс (путь до объекта);
- `<object_name>` — имя объекта с расширением.

Если указан относительный путь, при запросе объекта логика хранилища будет искать его с учетом префикса, указанного в запросе к контейнеру.

Например, если полный адрес объекта `<uuid>.selstorage.ru/container/prefix/file.html`, в качестве пути вы указали `file.html` и запрос выполняется по адресу `<uuid>.selstorage.ru/container/prefix/`, объект будет возвращен.

Например, если полный адрес объекта `<uuid>.selstorage.ru/container/prefix/file.html`, в качестве пути вы указали `prefix/file.html` и запрос выполняется по адресу `<uuid>.selstorage.ru/container/prefix/`, объект не будет возвращен, потому что логика хранилища будет искать объект по несуществующему адресу `<uuid>.selstorage.ru/container/prefix/prefix/file.html`.

CORS

При обращении к контейнеру браузер пользователя объявляет в запросе домен, метод запроса и заголовки. С помощью технологии кросс-доменных запросов (CORS) можно ограничить доступ к объектам в контейнере в зависимости от значений этих параметров.

Для использования CORS технология должна поддерживаться и хранилищем, и браузером пользователя, по умолчанию поддержка CORS включена в современные браузеры.

Для работы CORS должна быть включена Virtual-Hosted адресация.

Вы можете настроить конфигурацию CORS в панели управления или загрузить XML-файл конфигурации через S3 API.

Параметры CORS

Заголовок	Описание	Обязательный
AllowedOrigins	Перечень доменов, с которых разрешены запросы к контейнеру	✓
AllowedHeaders	Заголовки, доступные для использованияв JavaScript-приложении в браузере	✗
ExposeHeaders	Заголовки, разрешенные в запросе к объекту	✗
AllowedMethods	HTTP-методы, разрешенные для использования в запросах. Доступные методы: GET, PUT, HEAD, POST, DELETE	✓

MaxAgeSeconds	Время, в течение которого могут быть закешированы результаты Preflight request (в секундах). Если заголовок не указан, применяется значение по умолчанию — 3600	✗

Настроить конфигурацию CORS

Вы можете добавить до 100 правил CORS.

1. В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.
2. Откройте страницу контейнера → вкладка **CORS**.
3. Нажмите **Создать правило**.
4. Настройте параметры правила CORS.
5. Опционально: чтобы добавить еще одно правило, нажмите **Добавить правило**.
6. Нажмите **Создать**.

Удалить контейнер

Контейнеры, в которых находится не более 500 000 объектов (в том числе сегментов объектов), можно удалить через панель управления. Контейнеры с большим количеством объектов можно удалить только через API.

Удаление контейнера может занять до 24 часов. В процессе удаления с контейнером нельзя совершать никаких действий, кроме остановки удаления.

Если в контейнере включено версионирование, контейнер с версиями не удалится автоматически — его нужно удалить вручную.

Объекты в контейнере удаляются по очереди. Во время удаления контейнера исходящий трафик и объем хранения еще не удаленных объектов тарифицируются. Запросы DELETE не тарифицируются. Подробнее об оплате и потреблении в инструкции Модель оплаты и цены объектного хранилища.

Удалить контейнер

Перед удалением завершите все запросы к API с объектами в контейнере.

1. В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.
2. В строке контейнера нажмите 🗑️.
3. Введите имя контейнера и нажмите **Удалить**. В строке контейнера отобразится статус `Deleting`. После завершения удаления появится всплывающее уведомление.

Работа с объектами

Загрузить объект

Загружать объекты в контейнер можно двумя способами:

- простая загрузка доступна через панель управления и API. Ее можно использовать для файлов размером до 100 МБ. Мы не рекомендуем использовать кириллицу в именах объектов;
- сегментированная загрузка возможна только через Swift API и S3 API. Ее рекомендуется использовать для файлов размером более 100 МБ. Мы не рекомендуем использовать кириллицу в именах объектов.

Загрузить в контейнер можно любое количество объектов, если не установлены лимиты контейнера.

Простая загрузка

Если имя загружаемого объекта совпадает с именем объекта в контейнере, объект будет перезаписан.

1. В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.
2. Откройте страницу контейнера → вкладка **Объекты**.
3. Выберите объекты для загрузки.

Сегментированная загрузка

Сегментированная загрузка — это загрузка объектов по частям (сегментам), которую рекомендуется использовать для файлов размером более 100 МБ. Сегментированная загрузка возможна только через Swift API (технология SLO/DLO) и S3 API (технология Multipart Upload).

С ее помощью можно:

- загружать большие объекты сегментами меньшего размера;
- увеличить скорость загрузки объектов с помощью параллельных запросов;
- при сбоях в соединении не загружать объект заново, а повторять загрузку только нужных сегментов.

При загрузке объектов через API учитывайте ограничения объектного хранилища. Также учитывайте особенности удаления сегментированных объектов.

Скачать объект

1. В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.
2. Откройте страницу контейнера → вкладка **Объекты**.

3. Откройте страницу объекта.
4. В меню ⁝ объекта нажмите **Скачать**.

Удалить объект

В панели управления перейдите в раздел **Объектное хранилище** → **Контейнеры**.
Откройте страницу контейнера.
Откройте вкладку **Объекты**.
В меню ⁝ объекта нажмите **Удалить объект**.

1. Введите имя объекта и нажмите **Удалить**.
2. Если вы хотите удалить несколько объектов, отметьте каждый объект и нажмите **Удалить**.

Удалить сегментированный объект

При хранении объекта нельзя удалять его сегменты в служебном контейнере — это приведет к поломке всего файла.

Чтобы удалить объект с сегментами, удалите файл-манифест. Для удаления используйте API, которое вы использовали для загрузки объект. При удалении через панель управления используется Swift API.

Если загрузка и удаление объекта выполняется разными способами (например, объект был загружен с помощью S3 API, а удален в панели управления), сегменты объекта могут не удалиться, продолжить храниться в скрытом контейнере и тарифицироваться.