

Роли личного кабинета и их разрешения

Сразу после создания проекта в нем присутствует только один пользователь — его владелец. Владелец может пригласить в проект других участников, назначив им роли. Роль определяет список доступных разрешений при работе с функциональностью личного кабинета и с облачными сервисами.

Один и тот же пользователь может быть участником нескольких проектов и иметь в них разные роли. Одному участнику может быть назначено несколько ролей в одном проекте, в этом случае разрешения ролей суммируются.

Список участников проекта и назначенных им ролей можно посмотреть на странице **Управление доступами** личного кабинета.

Роли для общего управления проектом

Владелец проекта

Пользователь с максимально широким набором разрешений.

Владельцем становится пользователь, который создал проект, либо для которого проект был создан платформой при регистрации аккаунта.

В проекте может быть только один владелец. Эту роль нельзя назначить или пригласить на нее.

Администратор проекта

Пользователь, который имеет полные разрешения на создание и редактирование объектов во всех сервисах.

Администратор не может:

- активировать сервисы;
- пополнять баланс проекта (ему доступен только просмотр баланса);
- приглашать пользователей.

Администратор биллинга

Роль, предназначенная для управления балансом проекта.

Администратор биллинга может:

- привязать к проекту карту оплаты, если она еще не привязана;
- пополнить баланс проекта или настроить автопополнение.

Сервисы и список участников проекта этой роли недоступны.

Суперадминистратор

Пользователь, который имеет те же разрешения, что владелец, включая привязку карты и пополнение баланса.

Суперадминистратор — единственная роль, кроме владельца, которой доступна активация сервисов в проекте.

Администратор пользователей (IAM)

Роль, предназначенная для работы с участниками проекта на странице управления доступами.

Администратор пользователей (IAM) может приглашать участников в проект и удалять их из проекта, редактировать назначенные участникам роли.

Сервисы и информация о балансе проекта этой роли недоступны.

Наблюдатель

Пользователь, который имеет полные разрешения на просмотр информации в проекте, включая список участников, данные всех сервисов, баланс проекта и детализацию расходов.

Наблюдатель не может создавать какие-либо объекты и не может ничего редактировать, кроме настроек своего аккаунта.

Специализированные роли

Каждая из ролей ниже предназначены для работы с одним из сервисов платформы. Этим ролям доступны:

- разрешения в их целевом сервисе;
- ряд разрешений в сопутствующих сервисах, без которых невозможна полноценная работа с целевым сервисом.

У всех этих ролей отсутствует доступ к списку участников проекта и к информации о балансе.

Подробные сведения о разрешениях этих ролей в разделе [Матрица разрешений для всех ролей](#).

Все операции, доступные специализированным ролям, доступны также владельцу проекта, суперадминистратору и администратору проекта.

Администратор виртуальных машин

Пользователь с этой ролью может выполнять основные операции в сервисе Cloud Servers.

При этом ему доступен только просмотр для:

- планов резервного копирования;
- файловых хранилищ.

В сервисе виртуальных сетей он может создавать и редактировать группы правил (firewall).

Администратор сетевой безопасности

Пользователь с этой ролью может просматривать все данные в сервисах виртуальных сетей и DNS.

Создавать и редактировать он может только группы правил (firewall).

Администратор сети

Пользователь с этой ролью может выполнять полный набор операций в сервисах виртуальных сетей и DNS.

Администратор внутренних сетей

Пользователь с этой ролью может:

- просматривать все данные в сервисах виртуальных сетей и DNS;
- создавать и редактировать виртуальные сети и подсети, маршрутизаторы;
- добавлять в проект плавающие IP.

Администратор, оператор, аудитор Kubernetes

Подробная информация об этих ролях в разделе [Разрешения ролей сервиса Cloud Containers](#).

Матрица разрешений для всех ролей

Разрешения — это набор прав пользователей на просмотр (в таблице ниже — **R**) или изменение (**RW**) объектов. Разрешение на изменение объектов включает право на их создание и удаление, а также разрешение на просмотр. Отсутствие у роли доступа к сервису или функциональности обозначено прочерком (—).

Операции / Роль	Владелец проекта	Суперадминистратор	Администратор проекта	Наблюдатель	Администратор пользователей (AMU)	Администратор биллинга	Администратор виртуальных машин	Администратор сети	Администратор платимой функциональности	Администратор внутренних сетей	Администратор Kubernetes	Оператор Kubernetes	Аудитор Kubernetes
Общее управление													
Пользователи и их роли в проекте RW: добавление / удаление пользователей проекта, назначение им ролей. R: просмотр списка пользователей и их ролей	RW	RW	R	R	RW	—	—	—	—	—	—	—	—
Баланс и платежи RW: просмотр баланса проекта с детализацией расходов, пополнение баланса. R: просмотр баланса проекта без детализации расходов	RW	RW	R	R	—	RW	—	—	—	—	—	—	—
Виртуальные машины (Облачные вычисления)													
Виртуальные машины RW: добавление / изменение / удаление / перезагрузка VM, подключение VM к виртуальной сети, мониторинг VM, доступ к логам. R: просмотр и мониторинг VM, доступ к логам	RW	RW	RW	R	—	—	RW	—	R	R	—	—	—
Виртуальные диски RW: добавление / изменение / удаление дисков, мониторинг, создание снимков, миграция. R: просмотр дисков	RW	RW	RW	R	—	—	RW	—	R	R	—	—	—
Образы RW: добавление / изменение / удаление образов VM. R: просмотр образов	RW	RW	RW	R	—	—	R	—	R	R	R	—	—
Резервные копии RW: добавление / изменение / удаление списка резервного копирования и резервных копий, восстановление из резервных копий. R: просмотр списка резервного копирования, список резервных копий	RW	RW	RW	R	—	—	R	—	R	R	—	—	—
Файловые хранилища RW: добавление / изменение / удаление файловых хранилищ, управление правами доступа. R: просмотр файловых хранилищ, права доступа	RW	RW	RW	R	—	—	R	—	R	R	—	—	—
Сеть (Виртуальные сети и DNS)													
DNS-зоны RW: добавление / изменение / удаление DNS-зон. R: просмотр DNS-зон	RW	RW	RW	R	—	—	R	RW	R	R	R	R	R
Балансировщики нагрузки RW: добавление / изменение / удаление балансировщиков нагрузки. R: просмотр балансировщиков нагрузки	RW	RW	RW	R	—	—	R	RW	R	R	RW	R	R
Сети и подсети, IP адреса, маршрутизаторы RW: добавление / изменение / удаление сетей, подсетей, планировки IP-адресов, маршрутизаторов. R: просмотр сетей, подсетей, планировки IP-адресов, маршрутизаторов	RW	RW	RW	R	—	—	R	RW	R	RW	RW	R	R
VPN RW: добавление / изменение / удаление VPN-туннелей. R: просмотр VPN-туннелей	RW	RW	RW	R	—	—	R	RW	R	R	RW	R	R
Настройки firewall RW: добавление / изменение / удаление групп правил. R: просмотр групп правил	RW	RW	RW	R	—	—	RW	RW	RW	R	RW	R	R
Сервисы PaaS													
Контейнеры RW: добавление / изменение / удаление кластеров Kubernetes. R: просмотр кластеров Kubernetes	RW	RW	RW	R	—	—	—	—	—	—	RW	R	—
Мониторинг RW: добавление / изменение / удаление дашбордов и трекеров. R: просмотр дашбордов и трекеров	RW	RW	RW	R	—	—	RW	—	R	R	—	—	—
Все остальные сервисы RW: добавление / изменение / удаление объектов. R: просмотр объектов	RW	RW	RW	R	—	—	—	—	—	—	—	—	—

Разрешения ролей сервиса Cloud Containers

В личном кабинете доступны специализированные роли для работы с сервисом Cloud Containers:

- администратор Kubernetes,
- оператор Kubernetes,
- аудитор Kubernetes.

Операции, доступные администратору Kubernetes, доступны также владельцу проекта, суперадминистратору и администратору проекта.

Для остальных ролей эти операции недоступны.

Для кластеров Kubernetes версии 1.23 и выше роль администратора, оператора или аудитора Kubernetes также определяет доступную пользователю внутреннюю роль Kubernetes.



Некоторые действия доступны только в определенном состоянии кластера. Например, установка и удаление аддонов возможны, только если кластер запущен.

Операция/Роль	Администратор Kubernetes	Оператор Kubernetes	Аудитор Kubernetes	Наблюдатель
Создать кластер	✓	✗	✗	✗
Удалить кластер	✓	✗	✗	✗
Запустить кластер	✓	✓	✗	✗
Остановить кластер	✓	✓	✗	✗
Отобразить информацию о кластере, нод-группах	✓	✓	✓	✓
Получить kubeconfig	✓	✓	✓	✗
Получить секрет для доступа в Kubernetes Dashboard	✓	✓	✓	✓
Обновить версию	✓	✓	✗	✗
Изменить тип виртуальной машины	✓	✓	✗	✗
Изменить размер диска Prometheus	✓	✓	✗	✗
Добавить группу узлов	✓	✓	✗	✗
Удалить группу узлов	✓	✓	✗	✗
Изменить настройки масштабирования	✓	✓	✗	✗
Изменить Labels и Taints	✓	✓	✗	✗
Установить / удалить аддон	✓	✓	✗	✗