

CVAT roles

Содержание

1. Терминология
2. Админ-панель
3. Разметчик
 1. `Sandbox`
 1. без группы
 2. `user`
 3. `business`
 4. `admin`
 2. `Organization` 1.

Терминология

В разметке существует 2 типа рабочих областей:

- `Sandbox - Personal workspace` - пространство, в котором задачи отображаются на главной странице (не принадлежащие кастомным workspace'ам)
- `Organization` - пространство кастомного workspace
- `Admin page` - админ-панель
- `Cloud Storages` - облачные хранилища

Почитать про `Organization` можно тут: <https://openvinotoolkit.github.io/cvat/docs/manual/advanced/organization/>

Админ-панель

В админ-панели в разрешениях `Permissions` есть три поля

- `Active`
- `Staff status`
- `Superuser status`
- `Active` - убрав флаг аккаунт становится неактивным (альтернатива удалению). После отключения аккаунт не сможет авторизоваться в разметчике и админ-панели. Однако, при этом назначить на `job/task` и прочее этот аккаунт можно и он будет отображаться в списке предлагаемых
- `Staff status` - флаг, дающий право на авторизацию в админ-панели. При этом прав на редактирование информации нет. А объём отображаемой информации минимален
- `Superuser status` - флаг, дающий **полный** доступ к админ-панели. **НО** требует наличие флага `Staff status` (без него нельзя авторизоваться в админ-панели)

Разметчик

Sandbox

Для рабочей области `Sandbox` роли пользователям назначаются в админ-панели (`Admin page`). Во вкладке `groups` по умолчанию существуют 4 группы и 1 неявная (без принадлежности к какой-либо группе). Каждая последующая группа имеет права предыдущей + свои.

Примечание: в разделе `Groups` можно создавать свои группы и логически объединять пользователей. Дополнительных прав такие группы не дают. Однако, как пример использования, при работе с **API** по таким группам удобно находить нужных пользователей.

1. без группы
2. `worker`

3. `user`
4. `business`
5. `admin`

Доступ к `kibana` имеют пользователи с ролями `business` и `admin`

Organization

В этом разделе будут описаны только пользователи, добавленные в конкретную `Organization`. Недобавленные пользователи не имеют к ней доступа. Исключение - роль `admin`.

Важно знать! Один и тот же аккаунт можно добавлять в несколько организаций. Однако, добавив хотя бы в одну организацию, Вы лишаетесь возможности назначать этот аккаунт в рабочей области `Sandbox` используя интерфейс разметчика. Примечание: возможен обход этого ограничения - назначать с помощью `API`.

Внутри организации пользователи получают роли организации (дополнительно к ролям `Groups`). Таким образом доступ к тем или иным действиям определяется комбинацией роли `Groups` и роли выбранной `Organization`

Роли организации бывают:

1. `Worker`
2. `Supervisor`
3. `Maintainer`
4. `Owner`

Распределение прав

В файле **CVAT roles.xlsx** находится таблица, в которой отображена вся информация о том правах пользователей с теми или иными ролями.

| Scope | Resource | Context | Ownership | Privilege | Membership | Limit | Method | URL |
|-------|-----------|---------|-----------|-----------|------------|----------------------------------|--------|------------|
| view | Analytics | | | business | | resource['visibility']=='public' | GET | /analytics |
| view | Analytics | | | admin | | | GET | /analytics |

На примере прав `kibana` (Analytics) рассмотрим как пользоваться таблицей. Так выглядит фрагмент таблицы, показывающий, что доступ к `kibana` имеют пользователи с ролями `business` и `admin`

1. Scope - возможное действие
2. Resource - раздел, к которому будет применено действие
3. Context - рабочая область; возможные значения
 - пустое
 - `Sandbox`
 - `Organization`
4. Ownership - здесь указывается уровень владения (например у Task'a есть owner, assignee - это создатель и назначенный на task, у Job'a есть assignee - назначенный на job и т.д.)
5. Privilege - роль аккаунта, заданная ему в админ-панели
6. Membership - роль аккаунта, заданная ему в организации
7. Limit - ограничения в действиях
8. Method - метод API запроса (информация для разработчиков)
9. URL - url API запроса (информация для разработчиков)

Ещё один пример - кто может создавать новый task

| Scope | Resource | Context | Ownership | Privilege | Membership | Limit | Method | URL |
|--------|----------|---------|-----------|-----------|------------|--|--------|--------|
| create | Task | Sandbox | None | User | | resource['user'] ['num_resources'] < 10 | POST | /tasks |
| create | Task | Sandbox | None | Business | | | POST | /tasks |

| Scope | Resource | Context | Ownership | Privilege | Membership | Limit | Method | URL |
|--------|----------|--------------|-----------|-----------|------------|--|--------|--------|
| create | Task | Organization | None | User | Supervisor | resource['user'] ['num_resources'] < 10 | POST | /tasks |
| create | Task | Organization | None | Business | Supervisor | | POST | /tasks |

Если читать построчно то получается:

1. Создать task в Sandbox может аккаунт с ролью User (но только до 10 на аккаунт)
2. Создать task в Sandbox может аккаунт с ролью Business (тут уже без ограничений)
3. Создать task в Организации может аккаунт с ролью User и (одновременно) ролью организации Supervisor (но только до 10 на аккаунт)
4. Создать task в Организации может аккаунт с ролью Business и (одновременно) ролью организации Supervisor (тут уже без ограничений)

Примечание: т.к. каждая более старшая роль имеет права предыдущей + свои, именно поэтому роль `admin` в данной таблице не отображается