| **Название** | **Вес** |
| --- | --- |
| Аутентификация[[1]](#footnote-0) | 10 |

[**Внешняя vs. локальная аутентификация**](#_9w85qi5hcg25) **1**

[**Пользователи и группы**](#_4indqlbyfelo) **2**

[**Границы авторизации в Rancher**](#_ylmuaay7l6e8) **2**

[**Внешняя настройка аутентификации и пользователи-принципалы**](#_8xiglc6u3q9g) **4**

Одной из ключевых функций, которые Rancher добавляет в Kubernetes, является централизованная аутентификация пользователя. Эта функция позволяет вашим пользователям использовать один набор учетных данных для аутентификации в любом из ваших кластеров Kubernetes.

Эта централизованная аутентификация пользователя выполняется с помощью прокси-сервера аутентификации Rancher, который устанавливается вместе с остальной частью Rancher. Этот прокси-сервер проверяет подлинность ваших пользователей и пересылает их запросы в ваши кластеры Kubernetes, используя учетную запись службы.

# Внешняя vs. локальная аутентификация

Прокси-сервер аутентификации Rancher интегрируется со следующими внешними сервисами аутентификации.

| **Сервис аутентификации** |
| --- |
| Microsoft Active Directory |
| GitHub |
| Microsoft Azure AD |
| FreeIPA |
| OpenLDAP |
| Microsoft AD FS |
| PingIdentity |
| Keycloak (OIDC) |
| Keycloak (SAML) |
| Okta |
| Google OAuth |
| Shibboleth |

Однако Rancher также предоставляет локальную аутентификацию. В большинстве случаев вам следует использовать внешний сервис аутентификации вместо локальной аутентификации, поскольку внешняя аутентификация позволяет управлять пользователями из центрального размещения (central location). Однако в редких случаях вам может потребоваться несколько пользователей локальной аутентификации для управления Rancher, например, если ваш внешний поставщик аутентификации недоступен или проходит техническое обслуживание.

# Пользователи и группы

Rancher использует концепции пользователей и групп, чтобы определить, кому разрешено входить в Rancher и к каким ресурсам можно получить доступ. При аутентификации с помощью внешнего поставщика (external provider) группы предоставляются от внешнего поставщика на основе пользователей. Этим пользователям и группам назначаются определенные роли для таких ресурсов, как кластеры, проекты, многокластерные приложения, а также глобальные поставщики DNS и записи. Когда вы предоставляете доступ к группе, все пользователи, являющиеся членами этой группы в поставщике аутентификации, смогут получить доступ к ресурсу с указанными вами разрешениями. Дополнительные сведения о ролях и разрешениях см. в разделе "Управление доступом на основе ролей".

***Примечание:*** *Локальная аутентификация не поддерживает создание групп или управление ими.*

Дополнительные сведения см. в разделе Пользователи и группы.

# Границы авторизации в Rancher

После того, как в Rancher будет разрешен вход с использованием внешнего сервиса аутентификации, необходимо настроить, кому будет разрешено входить в систему и использовать Rancher. Доступны следующие опции:

| **Уровень доступа** | **Описание** |
| --- | --- |
| Allow any valid Users[[2]](#footnote-1) | Любой пользователь в сервисе авторизации может получить доступ к Rancher. Как правило, мы не рекомендуем использовать этот параметр! |
| Allow members of Clusters, Projects, plus Authorized Users and Organizations[[3]](#footnote-2) | Любой пользователь в сервисе авторизации и любая группа, добавленная в качестве **Cluster Member** (член кластера) или **Project Member** (участник проекта), могут войти в Rancher. Кроме того, любой пользователь сервиса аутентификации или группы, которую вы добавляете в список **Authorized Users and Organizations** (авторизованные пользователи и организации), может войти в Rancher. |
| Restrict access to only Authorized Users and Organizations[[4]](#footnote-3) | Войти в Rancher могут только пользователи сервиса аутентификации или группы, добавленные в **Authorized Users and Organizations** (авторизованные пользователи и организации). |

Чтобы установить уровень доступа Rancher для пользователей в сервисе авторизации, выполните следующие действия:

1. В верхнем левом угле нажмите **☰> Users & Authentication** (пользователи и аутентификация).
2. На левой панели навигации выберите **Auth Provider** (поставщик авторизации).
3. После настройки сведений о конфигурации для поставщика авторизации используйте параметры **Site Access** (доступ к сайту), чтобы настроить область авторизации пользователя. В таблице выше описан уровень доступа для каждого параметра.
4. Дополнительно: Если вы выберете параметр, отличный от **Allow any valid Users** (разрешить любым валидным пользователям), вы можете добавить пользователей в список **Authorized Users and Organizations** (авторизованные пользователи и организации), с помощью поиска их в появившемся текстовом поле.
5. Нажмите **Save** (сохранить).

**Результат:** Применены параметры конфигурации доступа Rancher.

{{< saml\_caveats >}}

# Внешняя настройка аутентификации и пользователи-принципалы

Для настройки внешней аутентификации требуются:

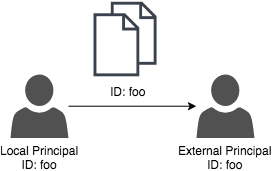
* локальный пользователь, которому назначена роль администратора, именуемый далее *локальным принципалом* (local principal);
* внешний пользователь, именуемый далее *внешним принципалом* (external principal), который может проходить аутентификацию с помощью вашего внешнего сервиса аутентификации.

Настройка внешней аутентификации влияет на то, как в Rancher происходит управление пользователями-принципалами. Для лучшего понимания изучите приведенный ниже список.

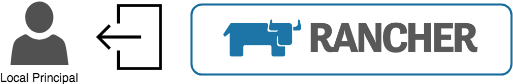
1. Войдите в Rancher в качестве локального принципала и завершите настройку внешней аутентификации.



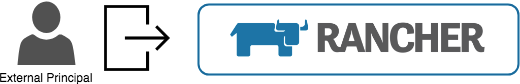
1. Rancher связывает внешнего принципала с локальным принципалом. Эти два пользователя совместно используют идентификатор пользователя локального принципала.



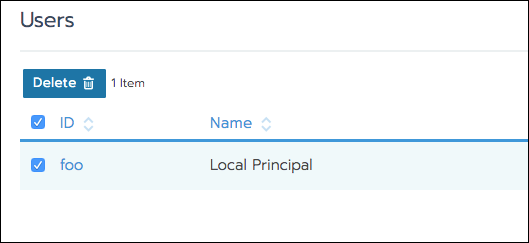
1. После завершения настройки Rancher автоматически выходит из локального принципала.



1. Затем Rancher автоматически вернет вас обратно в качестве внешнего принципала.



1. Поскольку внешний принципал и локальный принципал имеют общий идентификатор, на странице **Users** (пользователи) не отображается уникальный объект для внешнего принципала.



1. Внешний принципал и локальный принципал имеют одинаковые права доступа.

1. [Authentication](https://github.com/rancher/docs/blob/master/content/rancher/v2.6/en/admin-settings/authentication/_index.md) [↑](#footnote-ref-0)
2. разрешить любым валидным пользователям [↑](#footnote-ref-1)
3. разрешить участникам кластеров, проектов, а также авторизованным пользователям и организациям [↑](#footnote-ref-2)
4. ограничить доступ только для авторизованных пользователей и организаций [↑](#footnote-ref-3)