Контроль доступа с помощью списков доступа (ACL)

«Докувики», как и большинство других вики, по умолчанию очень открыто. Каждому позволено создавать, редактировать и удалять статьи. Однако, иногда имеет смысл ограничить доступ к определённым или всем статьям. Именно в этом случае «выходят на сцену» *списки доступа* (ACL). Данная статья делает обзор как ACL функционируют в «ДокуВики» и как их конфигурировать.

Предупреждение: Функционал ACL включён в «ДокуВики» достаточно давно и должен быть довольно стабилен. Однако, если вас особенно беспокоит риск того, что неавторизованные пользователи получат доступ к информации вашей вики, вы никогда не должны оставлять её на компьютерах, доступ к которым разрешён из открытого интернета…

Установка и конфигурация

ACL могут быть включены во время работы установщика и тогда будет установлена стандартная начальная политика ACL. Для ручного включения ACL установите опцию useacl и скопируйте файлы `conf/acl.auth.php.dist` и `conf/users.auth.php.dist` в `conf/acl.auth.php` и `conf/users.auth.php` соответственно.

Пример минимального файла `conf/users.auth.php` для пользователя `admin` с паролем `admin`. Если вы используете его, обязательно измените пароль после этого.

conf/users.auth.php

```
# Логин:Хэш пароля:Настоящее имя:email:Группы, через зяпятую

admin:$2y$10$P5YH8uIM2uAE9snRq32yAuHMb4/XAzksFd5Cakqqtsw9BWeSsyLZq:admin:admin@admin.com:admin,user
```

См. также

Есть ещё несколько опций конфигурации и функциональных свойств, относящихся к ограничениям прав пользователей и настройкам ACL. Пожалуйста, обратитесь к следующим статьям за более детальной информацией:

- Опция конфигурации useacl — разрешить ACL.
- Опция конфигурации superuser — назначение суперпользователей.
- Опция конфигурации disableactions — позволяет вам запретить открытую регистрацию.
- Опция конфигурации defaultgroup — группа, к которой по умолчанию приписывается новый пользователь.
- Менеджер пользователей — управление пользователями.
- Бэк-энды аутентификации — идентифицируют пользователей по разным источникам.

- FAQ: Как отключить открытую регистрацию пользователей.

Ограничение доступа

Ограничения доступа могут быть привязаны к статьям и пространствам имён.

Есть семь уровней доступа: *никаких (none)*, на *чтение (read)*, *изменение (edit)*, *создание (create)*, *загрузку (upload)*, *удаление (delete)* и *администрирование (admin)*.

У *«чтения»* самый низкий уровень доступа, у *«удаления»* — самый высокий. Если разрешён один уровень доступа (например, *создание*), то и все более низкие (*чтение* и *изменение*) так же разрешены. Следует отметить, что *«создание»*, *«загрузка»* и *«удаление»* относятся только к пространствам имён.

Правила, установленные для пространств имён, применяются и к пространствам имён медиафайлов точно также, как и к пространствам имён статей.

Когда система «ДокуВики» определяет права конкретного пользователя для доступа к конкретной статье, она выбирает из всего списка правил одно, согласно следующей процедуре:

- выбираются все правила, для которых выполняется условие <пользователь или группа>, т. е., либо имя пользователя совпадает с указанным, либо, если указана группа, то пользователь принадлежит этой группе. Остальные правила «выбрасываются» из рассмотрения.
- из оставшихся в рассмотрении выбирается правило, для которого наилучшим образом выполняется условие <`namespace:page`>, это мы называем specific matching (более специфичное совпадение).
- если в нескольких правилах происходит совпадение с условием <`namespace:page`> в одинаковой мере, то выбирается правило с наибольшим <уровнем доступа>.

Пользователи входят в группы, к которым они были приписаны менеджером пользователей (или бекэндом аутентификации). Однако есть две специальные **группы:**

- **@ALL**. Все пользователи, даже не совершившие вход в систему, являются членами группы ALL. Вы можете использовать эту группу для того, чтобы ограничить права для всех пользователей по умолчанию и ослабить это ограничение для нескольких выбранных пользователей.
- **@user**. Все пользователи, зарегистрировавшие себя, по умолчанию автоматически являются членами группы user. Используйте эту группу для назначения прав пользователям, совершившим вход в систему. Название данной группы задаётся в опции defaultgroup. В отличие от виртуальной группы ALL, user — это реальная группа, в которую автоматически добавляются все зарегистрированные пользователи при условии, что для авторизации используется plain backend. Если вы используете другой бэк-энд, вам нужно использовать группы предоставляемые этим бекэндом.

Представление групп внутри системы и в менеджере ACL отличается тем, что перед именем группы ставится символ «@».

Редактирование ACL

Наиболее простой способ добавить новое или отредактировать существующие правила, это использовать менеджер ACL, доступный из панели администратора. Доступно детальное описание этого интерфейса.

Обычно необходимо совершить три шага для добавления нового правила ACL:

1. выберите пространство имён или статью, на которые накладываются ограничения, из дерева навигации, расположенного вверху слева;
2. выберите, к кому это правило ACL должно применяться:
    - либо отметив уже существующего пользователя или группу из выпадающего меню;
    - либо выбрав тип (User: или Group:) и введя имя (пользователя или группы) в соответствующем поле;
3. установите подходящие права доступа.

Существующие правила могут быть изменены или удалены в таблице, приведенной внизу окна менеджера ACL.

Правила ACL в примерах

В этом разделе мы объясним как работают правила доступа, используя фиктивный пример настроек, которые в менеджере ACL выглядят следующим образом:

Рассмотрим каждую из строк:

1. Эта строка устанавливает права для всех в основном пространстве имён, позволяя каждому редактировать и создавать статьи. Однако загрузка файлов на сайт не разрешена.
2. Пользователю *bigboss* предоставлены все права.
3. Теперь доступ к пространству имён `devel` ограничен. Всем запрещено делать что-либо.
4. Ну хорошо, на самом деле, не всем — мы дали членам группы *devel* полные права здесь.
5. И конечно *bigbossy* тоже позволено — и он единственный, кто может удалять загруженные файлы.
6. А команда *marketing* может читать всё в пространстве имён, но только читать.
7. Однако ребята из `devel` не хотят, чтобы их босс видел статью `funstuff` — помните, что правило, точно соответствующее статье, «перебивает» правило, относящееся к пространству имён.
8. И, наконец, ребятам из группы *marketing* также позволено редактировать статью `devel:marketing`.
9. Далее установлены права для пространства имён `marketing`. Всем членам группы `marketing` позволено загружать сюда файлы
    - для остальных пользователей срабатывает правило **1,** поэтому они всё ещё могут создавать и редактировать статьи здесь.
    - *bigboss* наследует свои права из строки **2,** поэтому может загружать файлы сюда и удалять их.
10. Наконец, последняя строка ограничивает доступ к начальной статье для всех только на чтение, только суперпользователь может хотя бы редактировать её.

Давайте взглянем на второй пример, чтобы лучше понять **specific matching** (более специфичное совпадение):

На этот раз мы разберём, какие правила выберутся для разных пользователей при их попытке получить права к статье `private:bobspage`.

1. для обычного пользователя *abby*:
   - условие <пользователь или группа> выполняется в трёх правилах: №1, №2 и №4.
   - условие <`namespace:page`> лучше всего (другими словами: более конкретно) выполняется в правиле №4.
   - согласно правилу №4 уровень доступа пользователя *abby* к статье <`private:bobspage`> определяется 0, т. е. у *abby* нет никакого доступа к этой статье.
2. для обычного пользователя *bob*:
   - условие <пользователь или группа> выполняется в четырех правилах: №1, №2, №4 и №6.
   - условие <`namespace:page`> лучше всего выполняется в правиле №6. (Скажу больше, тут <`namespace:page`> **точно** совпадет со статьей)
   - уровень доступа *boba*: 16.
3. *bob* забыл войти в систему и пытается как неавторизованный пользователь получить доступ к своей статье:
   - условие <пользователь или группа> выполняется в двух правилах: № 1 и № 4.
   - условие <`namespace:page`> лучше всего выполняется в правиле № 4.
   - уровень доступа: 0.
4. для пользователя *charlie,* который входит в группу staff:
   - условие <пользователь или группа> выполняется в пяти правилах: с №1 по №5.
   - условие <`namespace:page`> лучше всего выполняется в двух правилах №4 и №5, но в правиле №5 <уровнем доступа> выше.
   - уровень доступа *charlie*: 16.

Заметим следующее: могло бы показаться, что правило №5 дублирует правило №3, но без пятого правила члены группы staff не получили бы доступ к пространству имён private, т. к. этому препятствовало бы правило №4.

Информация о внутреннем представлении ACL

Ограничения доступа хранятся в файле `conf/acl.auth.php`, который должен быть доступен для записи веб-серверу, если вы хотите использовать интерфейс администрирования ACL.

Не рекомендуется вручную править этот файл, вместо этого используйте интерфейс администратора.

Пустые строки и комментарии, начинающиеся с символа «#», игнорируются.

Каждая строка содержит три поля разделенных пробелами:

- Ресурс, на который накладывается ограничение. Это может быть статья или

пространство имён. Пространства имен отмечаются дополнительной звездочкой (см. пример ниже).
- Имя пользователя или группы. Имя группы отмечается символом «@» в начале.
- Уровень доступа (см. ниже).

Существует 7 уровней доступа. Они представляются целыми числами. Более высокий уровень включает в себя все более низкие. Если вы можете редактировать, то вы также автоматически можете читать. Есть уровень доступа *admin* (соответствует числу *255*), который никогда не должен использоваться в файле `conf/acl.auth.php`. Он используется только внутри системы при сравнении с опцией superuser.

Имя	Уровень	Применимо к...	Права доступа	Константа в исходниках «Докувики»
none	0	статьи, простр. имён	нет доступа — полный запрет	AUTH_NONE
read	1	статьи, простр. имён	право на чтение	AUTH_READ
edit	2	статьи, простр. имён	можно изменять существующие статьи	AUTH_EDIT
create	4	простространства имён	можно создавать новые статьи	AUTH_CREATE
upload	8	простространства имён	можно загружать медиафайлы	AUTH_UPLOAD
delete	16	простространства имён	можно заменять или удалять медиафайлы	AUTH_DELETE
admin	255	плагин admin	суперпользователь[1)] может изменять настройки	AUTH_ADMIN

Вот пример представления, которое совпадает с первым примером, приведённому выше:

```
*                    @ALL        4
*                    bigboss    16
devel:*              @ALL        0
devel:*              @devel      8
devel:*              bigboss    16
devel:*              @marketing  1
devel:funstuff       bigboss     0
devel:marketing      @marketing  2
marketing:*          @marketing  8
start                @ALL        1
```

Пожалуйста запомните, что **порядок не имеет значения.** Файл обрабатывается целиком, когда ищется наиболее подходящие правило для текущей связки «статья—пользователь». Если такое правило найдено, дальнейшие поиски прекращаются. Если не найдено, проводится проверка на совпадение связки «статья—группа» для всех групп, членом которых является текущий пользователь. Если и тут совпадений нет, то поиск проводится для следующего уровня пространства имён данной статьи. И т. д., пока не достигнем правила со связкой «*/@ALL».

Замечание: право на *удаление (delete)* относится только к медиафайлам. Статьи могут быть удалены (и восстановлены) любым пользователем, имеющим право на *редактирование (edit)*. Пользователь, у которого есть права на *загрузку (upload)*, но нет права на *удаление (delete)*, также не может переписать существующие медиафайлы.

Кодировка пользователя / группы

Если в имени пользователя или группы должны быть спецсимволы (такие, как пробел, например), то они (символы) должны быть преобразованы точно также, как они преобразуются в соглашениях об URL. Это относится только к спецсимволам с ASCII-кодами ниже 128. Файл ACL использует кодировку UTF-8, поэтому могут использоваться любые многобайтовые символы в том виде как они есть.

Пример: `Herbert.Müller` становится `Herbert%2eMüller`

(Это относится только к случаям, когда используется бэк-энд, отличный от «plain»; «plain backend» в любом случае не допускает спецсимволы нигде.)

Подстановки имён пользователей

Есть возможность использовать **подстановки имён пользователей** (user wildcards) в списках доступа. Это может быть полезным в вики с большим количеством зарегистрированных пользователей, если вы хотите дать каждому пользователю персональное пространство имён, в котором только он имел бы доступ на редактирование, и если вы не хотите при этом редактировать ACL для каждого пользователя. А достичь это позволяет то, что подстановка %USER% заменяется на имя пользователя, который в данный момент «залогинен» в системе и %GROUP% все группы этого пользователя.

В этом случае зарегистрированный пользователь имеет доступ только к собственному пространству имен и не имеет доступа к пространствам имен других пользователей (даже к просмотру названий пространств имен других пользователей).

Предоставить полный доступ к пространству имен пользователя, вошедшего всистему user:%USER%:* %USER% 16

Разрешить просматривать собственное пространство имен через «все страницы»: user: %USER% 1

Разрешить доступ только для чтения к странице «start», расположенной в пространстве имен «user» user: start %USER% 1

Отключить весь доступ к домашним пространствам имен пользователя, не принадлежащим зарегистрированному пользователю # (включая просмотр пространств имен через «все страницы») user:* @user 0

Разрешить членам «group» редактировать страницы в пространстве имен «group». # БУДЬТЕ ОСТОРОЖНЫ, если у вас есть пространство имен «user», все члены группы по умолчанию # получит к нему доступ, поскольку %GROUP% будет заменен буквально %GROUP%:* %GROUP% 2

Замечание: Не так давно для обозначения подстановок использовался символ «@» («собака»). В более новых версиях он заменен на «%» (процент). Если вы обновляетесь со старой версии, то вы должны привести установки ACL в соответствие с этим.

1)

См. superuser

From:
https://wwoss.ru/ - **worldwide open-source software**

Permanent link:
https://wwoss.ru/doku.php?id=wiki:acl

Last update: **2023/08/31 19:12**