Redmine - Feature #24808
OAuth2 support for Redmine API Apps (OAuth2 Provider)

2017-01-11 11:57 - Jan from Planio www.plan.io

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marius BALTEANU	**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:	5.0.0		
Resolution:			

Description

I think, we should make Redmine an OAuth2 provider, so that client apps using Redmine's API can ask users to authenticate rather than asking for an API key. Another goal would be to limit access to API client apps, so that not all apps gain access to the full scope of data a user has access to.

I'm working on this currently and I will hopefully be able to submit a patch soon. Here's a first screenshot:

redmine_oauth2_provider.png

History

#1 - 2017-01-18 17:57 - Jan from Planio www.plan.io

- File authorized_apps.png added

- File my_account.png added

- File auth_prompt.png added

- File apps.png added

- File 0001-Use-named-routes-for-search-in-base-layout.patch added

- File 0002-Prevent-hash-type-URLs-from-being-namespaced-in-Menu.patch added

- File 0003-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch added

- File 0004-Redmine-style-UI-for-Doorkeeper-OAuth2-provider.patch added

- File 0005-Add-optional-scope-parameter-to-Role-allowed_to.patch added

- File 0006-Use-Redmine-s-permissions-as-OAuth2-scopes.patch added

- Status changed from New to Needs feedback

- Assignee deleted (Jan from Planio www.plan.io)

The attached patch series implements full OAuth2 provider support for Redmine.

Background

OAuth2 is a widely adopted protocol for granting access to API client applications. More information can be found here:

- https://oauth.net/2/
- https://aaronparecki.com/2012/07/29/2/oauth2-simplified

Screenshots

Here are a few screenshots that show how it looks like:

apps.png
Admins are able to create/modify/delete OAuth2 client apps from the user interface.

redmine_oauth2_provider.png
OAuth2 App credentials are generated and can then be used in API clients.

auth_prompt.png
In order for an App to gain access to Redmine, it must ask the user for permission.

my_account.png

*Regular users are able to see which apps currently have access to their data from their **My Account** area.*

authorized_apps.png

Regular users are able to revoke access to individual apps.

Live Demo

We are providing a live demo server and client via these links:

https://server.redmine-oauth.planio.org

Username/Password is admin:oauth2. The content on this server will be reset every 60 minutes. Feel free to create your own OAuth2 applications via the Admin section, but please don't modify/delete the "Sinatra Client App".

https://client.redmine-oauth.planio.org

You can use this app to try out the authentication/authorization flow. Feel free to create your own user accounts on the Redmine server for this.

The /issues API will only work if the view_issues scope is requested. If only the standard scopes are requested, you will see an error here (on purpose).

Feel free to download the client app code from our Planio repository to try out everything locally.

The patch series

- 0001 changes the base layout to use named routes. The old hash-style routes (e.g. {controller => 'search', :action => 'index'}) would get namespaced when the layout is used in a namespaced controller in a plugin or engine which is the case with the Doorkeeper gem introduced later.
- 0002 changes the MenuManager in a similar way and prevents the rendered menu links from getting namespaced in the above scenario.
- 0003 adds the Doorkeeper Gem and integrates it with Redmine in the relevant places. You could apply patches 0001-0003 only to get functioning OAuth2 provider support already. In detail, what happens is:
  - Gemfile - Gem is added in
  - app/controllers/application_controller.rb - Doorkeeper is used as a new optional authentication mechanism that is tried when regular Redmine API auth fails
  - app/views/my/account.html.erb - Link to Doorkeeper's views for managing a user's authorized apps
  - config/initializers/doorkeeper.rb - Configure Doorkeeper so that it ties in with Redmine's user and admin authentication
  - config/routes.rb - Add Doorkeeper specific routes and root_url which is needed by it
  - db/migrate/20170107092155_create_doorkeeper_tables.rb - Migrations to add Doorkeeper tables
  - lib/redmine.rb - Link to Doorkeeper's views for managing available apps within the admin section
  - public/stylesheets/application.css - Icon for Apps
  - test/unit/lib/redmine/i18n_test.rb - Fix locale counting in tests because doorkeeper-i18n introduces languages unknown to Redmine
- 0004 - integrates Doorkeeper further by overriding all views with Redmine compatible markup and makes use of Redmine's deny_access and require_login methods which become available once the Doorkeeper controllers are set to inherit from Redmine's ApplicationController
- 0005 - changes Role#allowed_to? so that it can accept an optional scope parameter which can be an array of permission symbols that will be used as a logical AND filter.
- 0006 - Allows OAuth2 client apps to use Redmine permissions as Scopes in the sense of OAuth2. This way, admins and application developers can limit the abilities of client apps. An app will generally have *at most* the permissions defined by the App definition or as reqested by the app during the auhtorization step. Of course, the app will never have *more* permissions than the user is has requested authorization for would have in a normal interactive scenario.

Considerations

Why use Doorkeeper?

Implementing OAuth2 "by hand" seemed like re-inventing the wheel. Building and maintaining such security-critical code is both error-prone and non-trivial. The Doorkeeper Gem is the de-facto standard solution for implementing an OAuth2 provider in Rails. It's tried and tested, well-maintained and used by many high profile apps and services.

Integrating it with Redmine required only minor changes to Redmine's code base itself which should hopefully make maintenance of this functionality quite easy.

Why can only admins create apps?

The decision that only Redmine admins can add new API client applications is debatable, but it felt like the easiest solution for this first version. Allowing regular users to create apps would have required more overridden Doorkeeper controllers, new Redmine permissions (e.g. add_apps, view_apps, destroy_apps, etc.)

In addition to that, enabling/diasbling things like the REST API, JSONP support, etc. is currently also only available to admins, so I thought it would be consistent.

Some translations are missing! Where are the I18n keys?

At the moment, I've included them via the doorkeeper-i18n Gem. Technically, we could pull the locales in to Redmine's code base. However, – in the spirit of open source – I'd advcate in favor of keeping them in the external Gem and working with the Doorkeeper maintainers to improve them if needed. I've fixed twoissues with the locales already via pull requests and they were accepted rather quickly.

That's it for now. I am looking forward to your feedback!

#2 - 2017-01-26 09:57 - Marius BALTEANU

IMO, I think that the OAuth2.0 provider will be a great addition to Redmine and a feature that we'll use for sure at our future integrations with other apps.

What I like very much is the separation between the users and applications. Now we've some users named like "<application_name>-Generic User" used to authenticate the API calls. Having the possibility to define them as apps and manage their permissions from a different screen is very useful.

#3 - 2017-01-26 10:10 - Jan from Planio www.plan.io

- Description updated

#4 - 2017-01-28 18:59 - Jan from Planio www.plan.io

- File deleted (0003-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch)

#5 - 2017-01-28 18:59 - Jan from Planio www.plan.io

- File 0003-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch added

Slightly updated version of 0003, using wider columns for scopes

#6 - 2017-01-29 16:23 - Jan from Planio www.plan.io

- File deleted (0003-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch)

#7 - 2017-01-29 16:24 - Jan from Planio www.plan.io

- File 0003-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch added

And another fix.

#8 - 2017-02-08 01:24 - Akipii Oga

+1

#9 - 2017-07-17 19:20 - Cheyenne Wills

+1

What is the current "status" of this? Is this kind of planned for a future release?

We have two apps that could benefit by this (I've been looking at the redmine_oauth_provider plugin, but it appears that it doesn't work with the current level of Redmine).

#10 - 2018-03-15 10:01 - Stephane Evr

+1

#11 - 2019-05-12 23:30 - Peter Volkov

I think that "Needs feedback" is a wrong status here. According to #12827 this status means that this ticket is waiting for author's feedback, and such tickets are invisible for developers. Jan could you updated patchset and Status here?

#12 - 2019-05-15 15:25 - Jan from Planio www.plan.io

- Status changed from Needs feedback to New

I'm setting the status to **New** then, as requested. Ideally, we could get some more feedback from other contributors if the feature is desired and if yes, I'd be happy to rebase the patches on current trunk.

#13 - 2019-05-16 09:33 - Bernhard Rohloff

I think it can be a nice feature for Redmine and would make it much easier to manage things like bots, dashboards and applications of that kind. IMHO it's definitely worth a rebase.
+1

#14 - 2019-11-04 17:56 - James H

+1

#15 - 2019-12-12 03:24 - Keisuke Matsuura

+1

#16 - 2020-04-14 20:30 - Jan S

I'm also interested in this.

#17 - 2020-06-25 22:36 - J. Pablo Zebraitis

+1

#18 - 2020-07-21 13:06 - Jens Krämer

- File 0001-oauth-Use-named-routes-in-base-layout-and-account-si.patch added
- File 0002-oauth-Prevent-hash-type-URLs-from-being-namespaced-i.patch added
- File 0003-oauth-Add-OAuth2-provider-capability-using-doorkeepe.patch added
- File 0004-oauth-Redmine-style-UI-for-Doorkeeper-OAuth2-provide.patch added
- File 0005-oauth-Add-optional-scope-parameter-to-Role-allowed_t.patch added
- File 0006-oauth-Use-Redmine-s-permissions-as-OAuth2-scopes.patch added

- File 0007-oauth-adds-system-test-to-test-the-oauth-provider-ca.patch added

I rebased this patch on current master and added a brief system test that covers application creation, authorization and usage with an actual oauth2 client.

I'd also like to add that, since a few weeks, we're using this feature successfully at Planio for authenticating the native Planio Storage client apps.

#19 - 2020-07-21 13:17 - Jan from Planio www.plan.io

- Target version set to Candidate for next minor release

Thanks Jens. I would really enjoy seeing this making its way into a future Redmine release and I believe it will help Redmine get more third party apps and integrations!

#20 - 2020-08-27 05:07 - Jens Krämer

- File 0001-Use-named-routes-in-base-layout-and-account-sidebar.patch added
- File 0002-Prevent-hash-type-URLs-from-being-namespaced-in-Menu.patch added
- File 0003-Add-optional-scope-parameter-to-Role-allowed_to.patch added
- File 0004-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch added

Another update to this patch. Notable changes are:

- updated to Doorkeeper 5.4, which allowed for the following improvements:
  - secrets (tokens, application secret) are now stored as hashes
  - support for PKCE (most relevant for non-confidential clients)
- introduced an admin scope which allows Administrators to grant admin permissions to client applications
- fixed a stored CSRF vulnerability that was present in one of the original Doorkeeper templates. It was only exploitable by Administrators but if you're using an older version of this patch, at least update your views according to this doorkeeper commit

We also just released the omniauth-redmine-oauth2 gem (source code at Planio and Github). We also built a small Rails app to demonstrate usage of the gem .

Currently this patch makes two I18n tests fail. This is due to the inclusion of the doorkeeper-i18n gem, which introduces 4 locales that aren't present in Redmine. In general, we would need to decide if we want to include these 3rd party translation at all (they do not cover all of Redmine's locales by a large margin) or if we incorporate them into Redmine. As of now the patch just overrides a few strings to make the wording more Redmine-like.

Due to the Doorkeeper upgrade I was more or less forced to squash the last 4 commits of the previous patch series, so it's down to 4 commits now.

#21 - 2021-02-25 00:22 - Marius BALTEANU

- Target version changed from Candidate for next minor release to Candidate for next major release

Jens, I've started to look to the provided patches and to test this feature. For now, I've committed all 4 patches to the Gitlab instance in order to get the tests results. Besides the I18n test fails, there are some Rubocop warnings that should be fixed.

Am I wrong if I say that patches 0001 and 0002 can be extracted from this issue and delivered as separated ticket? In this way, we will down this feature to 2 patches and it will be easier to maintain/rebase it.

I've assigning this to the next major release version because the changes are too huge for a minor version.

#22 - 2021-04-12 12:08 - Jens Krämer

thanks for looking into this! I just created #35075 and #35076 with the first two patches of this series. Both should not cause test failures or rubocop warnings. I'll look into these next and update this issue accordingly.

#23 - 2021-04-12 12:16 - Jan from Planio www.plan.io

Thanks Marius for looking into this. I think it should greatly improve the Redmine API to use state of the art authorization!

#24 - 2021-04-13 08:33 - Jens Krämer

- File 0003-Add-optional-scope-parameter-to-Role-allowed_to.patch added

- File 0004-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch added

here are the remaining two patches, updated to the most recent doorkeeper release (5.5.1), rebased on current master, and hopefully with a lot less rubocop warnings.

#25 - 2021-06-09 21:29 - James H

+100000000000000

#26 - 2021-06-25 00:34 - Marius BALTEANU

- Assignee set to Marius BALTEANU

- Target version changed from Candidate for next major release to 5.0.0

Files

redmine_oauth2_provider.png	330 KB	2017-01-11	Jan from Planio www.plan.io
my_account.png	80.6 KB	2017-01-18	Jan from Planio www.plan.io
authorized_apps.png	206 KB	2017-01-18	Jan from Planio www.plan.io
auth_prompt.png	218 KB	2017-01-18	Jan from Planio www.plan.io
apps.png	261 KB	2017-01-18	Jan from Planio www.plan.io
0001-Use-named-routes-for-search-in-base-layout.patch	2.83 KB	2017-01-18	Jan from Planio www.plan.io
0002-Prevent-hash-type-URLs-from-being-namespaced-in-Menu.patch	2.03 KB	2017-01-18	Jan from Planio www.plan.io
0004-Redmine-style-UI-for-Doorkeeper-OAuth2-provider.patch	15.7 KB	2017-01-18	Jan from Planio www.plan.io
0005-Add-optional-scope-parameter-to-Role-allowed_to.patch	4.27 KB	2017-01-18	Jan from Planio www.plan.io
0006-Use-Redmine-s-permissions-as-OAuth2-scopes.patch	7.87 KB	2017-01-18	Jan from Planio www.plan.io
0003-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch	9.81 KB	2017-01-29	Jan from Planio www.plan.io
0001-oauth-Use-named-routes-in-base-layout-and-account-si.patch	4.39 KB	2020-07-21	Jens Krämer
0002-oauth-Prevent-hash-type-URLs-from-being-namespaced-i.patch	2.04 KB	2020-07-21	Jens Krämer
0003-oauth-Add-OAuth2-provider-capability-using-doorkeepe.patch	10.1 KB	2020-07-21	Jens Krämer
0004-oauth-Redmine-style-UI-for-Doorkeeper-OAuth2-provide.patch	15.6 KB	2020-07-21	Jens Krämer
0005-oauth-Add-optional-scope-parameter-to-Role-allowed_t.patch	4.23 KB	2020-07-21	Jens Krämer
0006-oauth-Use-Redmine-s-permissions-as-OAuth2-scopes.patch	10.1 KB	2020-07-21	Jens Krämer
0007-oauth-adds-system-test-to-test-the-oauth-provider-ca.patch	4.68 KB	2020-07-21	Jens Krämer
0002-Prevent-hash-type-URLs-from-being-namespaced-in-Menu.patch	2.03 KB	2020-08-27	Jens Krämer
0001-Use-named-routes-in-base-layout-and-account-sidebar.patch	4.38 KB	2020-08-27	Jens Krämer

0003-Add-optional-scope-parameter-to-Role-allowed_to.patch	4.22 KB	2020-08-27	Jens Krämer
0004-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch	42.1 KB	2020-08-27	Jens Krämer
0003-Add-optional-scope-parameter-to-Role-allowed_to.patch	4.22 KB	2021-04-13	Jens Krämer
0004-Add-OAuth2-provider-capability-using-doorkeeper-gem.patch	42.2 KB	2021-04-13	Jens Krämer