Does Rails come with a "not authorized" exception?

Ask Question

Asked 10 years, 1 month ago Modified 2 years, 11 months ago Viewed 33k times

40

I am writing an application that uses plain old Ruby objects (POROs) to abstract authorization logic out of controllers.

Currently, I have a custom exception class called `NotAuthorized` that I `rescue_from` at the controller level, but I was curious to know: **Does Rails 4 already come with an exception to indicate that an action was not authorized?** Am I reinventing the wheel by implementing this exception?

Clarification: The `raise AuthorizationException` is not happening anywhere inside of a controller, it is happening inside of a completely decoupled PORO outside of the controller. The object has no knowledge of HTTP, routes or controllers.

ruby-on-rails ruby actioncontroller

Share
Improve this question
Follow

edited Sep 17, 2014 at 14:13

asked Sep 17, 2014 at 13:38
Rick
8,776 ● 9 ● 50 ● 78

well the http error code 401 means unauthorized, you could tell rails to return a 401 status code, and render whatever view you want – Mohammad AbuShady Sep 17, 2014 at 13:58

1 @MohammadAbuShady - I believe he's looking for sth like `raise ActionController::RoutingError.new('Not Found')` which automatically forces application to render 404 without any rescue statmenets. – BroiSatse Sep 17, 2014 at 14:08

2 I usually just use devise + cancan, a nice combination for authentication and authorization – Mohammad AbuShady Sep 17, 2014 at 14:09

3 Agree with @MohammadAbuShady but, if you go that route, make sure it's CanCanCan since CanCan has been abandoned :)! – craig.kaminsky Sep 17, 2014 at 14:18

Add a comment

2 Answers

Sorted by: Highest score (default)

38

Rails doesn't seem to map an exception to `:unauthorized`.

The default mappings are defined in activerecord/lib/active_record/railtie.rb:

```
config.action_dispatch.rescue_responses.merge!(
  'ActiveRecord::RecordNotFound'   => :not_found,
  'ActiveRecord::StaleObjectError' => :conflict,
  'ActiveRecord::RecordInvalid'    => :unprocessable_entity,
  'ActiveRecord::RecordNotSaved'   => :unprocessable_entity
)
```

and actionpack/lib/action_dispatch/middleware/exception_wrapper.rb:

```
@@rescue_responses.merge!(
  'ActionController::RoutingError'             => :not_found,
  'AbstractController::ActionNotFound'         => :not_found,
  'ActionController::MethodNotAllowed'         => :method_not_allow
  'ActionController::UnknownHttpMethod'        => :method_not_allow
  'ActionController::NotImplemented'           => :not_implemented,
  'ActionController::UnknownFormat'            => :not_acceptable,
  'ActionController::InvalidAuthenticityToken' => :unprocessable_en
  'ActionDispatch::ParamsParser::ParseError'   => :bad_request,
  'ActionController::BadRequest'               => :bad_request,
  'ActionController::ParameterMissing'         => :bad_request
)
```

You could add a custom exception from within your application's configuration (or a custom Railtie):

```
Your::Application.configure do

  config.action_dispatch.rescue_responses.merge!(
    'AuthorizationException' => :unauthorized
  )

  # ...

end
```

Share Improve this answer Follow

answered Sep 17, 2014 at 15:13
Stefan
114k ● 14 ● 156 ● 227

1 Thank you for answering my question. I am curious how exceptions are mapped with Mongoid as the ORM. – Rick Sep 17, 2014 at 15:27

1 @Stefan's link references a specific line number in `master` which changes over time. Here's a more "perma" link to that code: github.com/mongoid/mongoid/blob/v4.0.2/lib/mongoid/... – Luke Griffiths Jan 13, 2016 at 22:02

Add a comment

30

I'm guessing the reason Rails didn't introduce this exception is because Authorisation and Authentication is not Rails native behavior (not considering basicauth of course).

Usually these are responsibilities of other libraries Devise for NotAuthenticated; Pundit, Dude Policy, CanCanCan, Rollify for NotAuthorized) I would actually argue it may be a bad thing to extend `ActionController` with custom exceptions like `ActionController::NotAuthorized` (because like I said it's not it's responsibility)

So Way how I usually tackled this problem is that I've introduced custom exceptions on `ApplicationController`

```
class ApplicationController  < ActionController::Base
  NotAuthorized = Class.new(StandardError)
  # ...or if you really want it to be ActionController
  # NotAuthorized = Class.new(ActionController::RoutingError)

  rescue_from ActiveRecord::RecordNotFound do |exception|
    render_error_page(status: 404, text: 'Not found')
  end

  rescue_from ApplicationController::NotAuthorized do |exception|
    render_error_page(status: 403, text: 'Forbidden')
  end

  private

  def render_error_page(status:, text:, template: 'errors/routing')
    respond_to do |format|
    end
  end
end
```

Therefore in my controllers I can do

```
class MyStuff < ApplicationController
  def index
    if current_user.admin?
      # ....
    else
      raise ApplicationController::NotAuthorized
    end
  end
end
```

This clearly defines that the layer your expecting this exception to be raised and caught is your application layer, not 3rd party lib.

The thing is that libraries can change (and yes this means Rails too) defining exception on a 3rd party lib classes and rescuing them in your application layer is really dangerous as if the meaning of exception class changes it brakes your `rescue_from`

You can read lot of articles where people are Waring about Rails `raise` - `rescue_from` being the modern `goto` (now considering anti-pattern amongst some experts) and in certain extend it is true, but only if you are rescuing Exceptions that you don't have full control off !!

That means 3rd party exceptions (including Devise and Rails to certain point). If you define the exceptions classes in your application, you are not relaying on 3rd party lib => you have full control => you can `rescue_from` without this being an anti-pattern.

Share
Improve this answer
Follow

edited Nov 11, 2021 at 11:08

answered Jul 27, 2016 at 15:28
equivalent8
14.2k ● 8 ● 86 ● 114

Add a comment

Your Answer

Sign up or log in

Sign up using Google

Sign up using Email and Password

Post as a guest

Name

Email

Required, but never shown

Post Your Answer

By clicking “Post Your Answer”, you agree to our terms of service and acknowledge you have read our privacy policy.

Not the answer you're looking for? Browse other questions tagged **ruby-on-rails** **ruby** **actioncontroller** or ask your own question.

The Overflow Blog

- How can you get your kids into coding? We asked an 8-year-old app builder.
- Life in the Fastlane: SDK tools built with developers in mind

Upcoming initiatives on Stack Overflow and across the Stack Exchange network...

Call for testers for an early access release of a Stack Overflow extension...

Proposed designs to update the homepage for logged-in users

Linked

-1	Bitpay Ruby client funtion error

Related

1	restful_authentication: authorized? = NoMethodError (but logged_in? works fine...?)
2	Rails - authenticate_or_request_with_http_basic custom "access denied" message
2	Rails user authorization
0	Rails authentication not reacting to wrong username or password
0	Following The Rails getting Started Guide and getting a ActionController::InvalidAuthenticityToken
19	Respond with a status unauthorised (401) with Rails 4
0	How to fix Insufficient Authorization in Rails?
0	Rails controller: authenticating only for certain actions
6	Rails: Completed 401 Unauthorized
3	Rails: send a 401 error without rendering a page

Hot Network Questions

- Would a torchship be legal?
- Has "optimism in reason" been explicitly discussed as a philosophical position?
- Consciousness: irreducible phenomenon caused by physical processes
- What are the advantages and disadvantages of signing international protocols?
- UK visitor visa financial circumstance
- Does Occam's Razor favor metaphysical solipsism?

- How might communications on Mars work between bases if humans were there?
- A Simplification of the computation of local heights in Gross-Zagier
- Toy proof assistants with very small codebases
- One number placed in 3 places makes these equations correct
- Is a "hot cube" (analogous to an ice cube) a physical possibility?
- Is it appropriate to acknowledge your family or even mention them in articles or slideshows?
- What aircraft has the propeller with the highest blade count?
- Locally warping space so Earth turns "inside out" and engulfs the moon
- Short story about huge computer that answered philosophical questions. Preceded 'Deep Thought'
- Can a company be fined in a value larger than the global GDP?
- Is it possible for a voter to be rendered ineligible in both their prior and new states while in the process of moving?
- What is the definition of Force?
- VWP for residents of non-VWP countries
- When should I use a std::inplace_vector instead of a std::vector?
- Where did Anna Akhmatova write, "Half of the country imprisoning, half of the country imprisoned"?
- Rearranging terms of polynomials according to the constant coefficients

Question feed

STACK OVERFLOW

Questions Help Chat

PRODUCTS

Teams Advertising Talent

COMPANY

About Press Work Here Legal Privacy Policy Terms of Service Contact Us Cookie Settings Cookie Policy

STACK EXCHANGE NETWORK

Technology Culture & recreation Life & arts Science Professional Business API Data stack**overflow** Products

Log in Sign up