Redmine - Feature #35787
add IP address to "401 Unauthorized" log messages

2021-08-20 13:30 - Dietrich Streifert

Status:	Needs feedback	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Dietrich Streifert	**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

Hi all,

I'm in need to add a fail2ban filter/jail which allows blocking of IPs trying to use the REST api unauthorized.

Currently redmine logs this attempts like this:

```
2021-08-20 13:18:43 +0200 (185) Completed 401 Unauthorized in 4ms (ActiveRecord: 1.5ms)
```

which is not sufficient for fail2ban filters, because the IP address is missing.

It would be nice to additionally display the requesting IP in that log line, e.g.:

```
2021-08-20 13:18:43 +0200 (185) Completed 401 Unauthorized in 4ms (ActiveRecord: 1.5ms) from 1.2.3.4
```

This way it would be possible to write a filter usable for fail2ban.

History

#1 - 2021-08-20 13:36 - Stefan Lindner

+1

#2 - 2021-08-21 04:08 - Go MAEDA

I don't think we have to implement the feature. By adding the following line to config/additional_environment.rb, the client's IP address will be recorded in every line of the log.

```
config.log_tags = config.log_tags.to_a + [:remote_ip]
```

The log looks as follows.

```
[127.0.0.1] Started GET "/login" for 127.0.0.1 at 2021-08-21 10:26:35 +0900
[127.0.0.1] Processing by AccountController#login as HTML
[127.0.0.1]   Current user: anonymous
[127.0.0.1]   Rendered account/login.html.erb within layouts/base (Duration: 8.7ms | Allocations: 1435)
[127.0.0.1]   Rendered layout layouts/base.html.erb (Duration: 34.1ms | Allocations: 6278)
[127.0.0.1] Completed 200 OK in 47ms (Views: 34.7ms | ActiveRecord: 2.8ms | Allocations: 8520)
```

#3 - 2021-08-22 10:02 - Mischa The Evil

- Status changed from New to Needs feedback

- Assignee set to Dietrich Streifert

Can you all please provide some feedback following Go's suggestion?

#4 - 2021-08-24 09:34 - Dietrich Streifert

Thank you for your feedback and suggestion.

I tried Go's suggestion but it does not work. I've added exactly the line into config/additional_environment.rb but the IP address does not show up in the log.

My setup is a docker compose stack using the docker image redmine:4-passenger currently running redmine version 4.1.1.stable where I'm using the log file /usr/src/redmine/log/passenger.3000.log.

I've added the line suggested by Go into config/additional_environment.rb and mapped that file to /usr/src/redmin/config/additional_environment.rb added permissions and file ownership par to config/environment.rb, checked if the setting are there from whithin the running container. Now the content of config/additional_environment.rb is as follows:

```
config.logger = Logger.new(STDOUT)

config.log_tags = config.log_tags.to_a + [:remote_ip]
```

I've managed to add some code in config/environment.rb changing the timestamp in the log lines via

```
class Logger
  def format_message(severity, timestamp, progname, msg)
    "#{timestamp} (#{$$}) #{msg}\n"
  end
end
```

which works as expected.

Currently, with the addition from Go in config/additional_environment.rb, the log output in passenger.3000.log looks like this:

```
App 199 output: 2021-08-24 09:31:06 +0200 (199) Started GET "/users/current.xml" for 136.243.54.73 at 2021-08-24 09:31:06 +0200
App 199 output: 2021-08-24 09:31:06 +0200 (199) Processing by UsersController#show as XML
App 199 output: 2021-08-24 09:31:06 +0200 (199)   Parameters: {"id"=>"current"}
App 199 output: 2021-08-24 09:31:06 +0200 (199) User find_by_api_key 'dfasdfasdfasdf' gefunden: ''
App 199 output: 2021-08-24 09:31:06 +0200 (199)   Current user: anonymous
App 199 output: 2021-08-24 09:31:06 +0200 (199) Filter chain halted as
#<Proc:0x0000564c7bb5e460@/usr/src/redmine/app/controllers/users_controller.rb:25 (lambda)> rendered or redirected
App 199 output: 2021-08-24 09:31:06 +0200 (199) Completed 401 Unauthorized in 9ms (ActiveRecord: 3.7ms)
```

#5 - 2021-08-24 10:02 - Dietrich Streifert

Some additional note:

From my point of view adding the IP to every log line is problematic with respect to the GDPR in Europe, as it is not necessary to log the IP for every single action.

In situations where someone tries to log in or access resources without authorization, it is necessary to know the IP address in order to take action, such as blocking the potential attacker via the firewall.

So having the IP address logged only in this specific situation would be the far better solution.