redmineorg-copy202205 - Vote #74721

Possibility to limit user access to certain IPs and access method (Web or API)

2022/05/09 17:09 - Admin Redmine

ステータス:	New	**開始日:**	2022/05/09
優先度:	通常	**期日:**	
担当者:		**進捗率:**	0%
カテゴリ:	Security_51	**予定工数:**	0.00時間
対象バージョン:		**作業時間:**	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/15707	**status_id:**	1
category_id:	51	**tracker_id:**	2
version_id:	0	**plus1:**	1
issue_org_id:	15707	**affected_version:**	
author_id:	31099	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	10		

説明

There should be a possibility to limit the access of users to certain IP addresses and/or limit to either connect via browser or via API. This is especially interesting for the admin user.

Why?

We have e.g. an admin user, which is used for a bot connecting to redmine; to increase security I would like to limit this bot to access only via the REST API and from a certain host.

journals

What is difference with webserver (apache etc.) configuration?

The webserver does not have a concept about the user that is targeted within redmine. Lets fix an example:

I have the redmine admin user, having admin rights, thus capable of executing anything. Also I have a simple user "user" without admin rights. I know that I am the only person that is using the admin user, and that I am always connecting from 1.1.1.1. Thus, to enhance security, I would like Redmine to be capable of limiting the access of the admin user to queries coming from 1.1.1.1.

The webserver can not block this, as he has no knowledge about the user, and its limitations.

Same should go for the differentiation of Web-base and REST access. So I could create an "Admin Bot" allowing Rest only access from a certain IP as I know, there is no human to use the interface via browser.

Are you okay with this explanation?

+1

my opinion is that will be a plugin.

one or more Subnet definition(s) in Administrative Settings for restrict to internal access,

A checkbox on project settings for enable access from outside of local subnet (defined #1)

A checkbox on user profile for enable access from outside of local subnet

One or more IP/Subnet definition(s) in user profile for restrict internet access

If 3 is checked, 4 is active. If 3 is checked and 4 is empty, user can access from the all of the world if 2 is also active.

Best Regards,
Adnan

I am against the realization as a plugin. Security should be embedded deep in the core of the system, and a feature like this should be developed by the core developers in order to provide the required amount of security. I am not familiar with ruby development, however, how probable is it, that if this feature is realized as plugin it is capable by another plugin to circumvent the security measures?

AFAIK the code has to go deep into the first handler of incoming REST and Web requests, where all other stuff goes second; is it at all possible to hook a plugin at this specific point?

The following features would have to be realized:

- Allow to define per user what access method is applicable, where the possible access methods are ** Web Browser Interface ** REST

* Allow to define per user one or more subnet masks where the access may originate from, any access that does not originate from one of the given addresses should be answered with access denied.

Does anybody care about this issue? :(

Г о р д е е в А л е к с е й wrote:

> Does anybody care about this issue? :(

I suggest using this plugin: https://github.com/redmica/redmine_ip_filter

We sponsored the creation of an additional plugin for this a few years ago. See
https://github.com/MEDEVIT/redmine_access_filters

The fork in https://github.com/ngiger/redmine_access_filters works against redmine 4.1

Marco Descher wrote:

> The fork in https://github.com/ngiger/redmine_access_filters works against redmine 4.1

I haven't looked deeply into this, but commit "a0373b34574a72f6e83054c3c5662c2e9b634da5": https://github.com/ngiger/redmine_access_filters/commit/a0373b34574a72f6e83054c3c5662c2e9b634da5 comments-out the old @before_filter@ calls without any replacement. So this fork might not be functioning as expected.

Hey Mischa, thanks a lot for your comment - we'll look into this!

履歴

#1 - 2022/05/10 17:11 - Admin Redmine

- カテゴリ を Security_51 にセット