Smart Proxy - Bug #14153

Allow to run smart-proxy under passenger 5 with nginx

03/11/2016 04:15 AM - Mateusz Gozdek

Status:	Rejected		
Priority:	Normal		
Assignee:			
Category:	SSL		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

In passenger 5, they changed nginx config syntax from **passenger_set_cgi_param** to **passenger_set_header** and **passenger_env_var**. In passenger 4 we set

```
passenger_set_cgi_param         SSL_CLIENT_CERT $ssl_client_cert;
```

to authorize SSL access to foreman-proxy. In passenger 5 this is unfortunately impossible, because **passenger_env_var** is resolved only during application startup, **passenger_set_header** is adding **HTTP_ prefix** to each header, and because **SSL_CLIENT_CERT** header name is hardcoded in **lib/sinatra/authorization.rb** and **lib/proxy/helpers.rb**, we are not able to set proper header for authorization. Problem doesn't exists in **apache2**, because there is **+ExportCertData** option, which adds headers properly.

As a quick fix, I would suggest to allow to change **SSL_CLIENT_CERT** header name in **settings.yaml** file, with default value as **SSL_CLIENT_CERT**, to not affect current users.

Another, and in my opinion better solution would be to **change SSL validation mechanism** to same as in **foreman**, that is to make certificate validation on webserver site, and only validate if

```
SSL_CLIENT_VERIFY == SUCCESS
```

. And about validation **trusted_hosts**, we can extract client hostname from **SSL_CLIENT_S_DN**, to avoid parsing whole SSL certificate.

Suggesten nginx config part:

```
  passenger_set_header  X-SSL-Client-S-DN $ssl_client_s_dn;
  passenger_set_header  X-SSL-Client-Verify $ssl_client_verify;
```

to set **HTTP_X_SSL_CLIENT_S_DN** and **HTTP_X_SSL_CLIENT_VERIFY** headers to validate.

History

#1 - 03/11/2016 04:18 AM - Dominic Cleal

- Category set to SSL

#2 - 03/11/2016 05:22 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/smart-proxy/pull/392 added

#3 - 03/11/2016 05:25 AM - Mateusz Gozdek

I created pull request with fix. https://github.com/theforeman/smart-proxy/pull/392

#4 - 03/11/2016 06:03 AM - Anonymous

The alternative approach you suggested can be an option, but cannot be the sole way of performing client cert validation: it is pretty common to run smart-proxy directly on webrick.

#5 - 03/11/2016 08:47 AM - Mateusz Gozdek

You are right. I checked and webrick is passing only request with valid client certificate, which is correct. So our job is just to extract cn from client certificate. I think we can use **HTTP_X_SSL_CLIENT_S_DN** if it's not empty, otherwise, we will extract CN from certificate.

#6 - 01/29/2019 02:06 PM - Lukas Zapletal

- Status changed from Ready For Testing to Rejected

- Triaged changed from No to Yes

- Pull request deleted (https://github.com/theforeman/smart-proxy/pull/392)

The PR https://github.com/theforeman/smart-proxy/pull/392 did not make it. Feel free to reopen.