Installer - Bug #11652

Foreman installer sets Apache2 SSLCACertificatePath to system Trust Store

09/02/2015 05:08 AM - Arnd Hannemann

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	Foreman modules		
Target version:	1.11.0		
Difficulty:	easy	**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

The SSLCACertificatePath of the foreman ssl and puppet master vhost is set to the System Trust Store.
On debian this is:

```
SSLCACertificatePath    "/etc/ssl/certs"
```

So every user of a certificate issued by one of these CAs (there are many) can be successfully authenticate
against this apache installation.

Per Default foreman and the puppet master should really only trust his own CA (SSLCACertificateFile).
SSLCACertificatePath should not be set.

I verified this bug, by using an S/MIME valid certificate which I imported into my browser and then calling the Foreman ENC.
Luckily Foreman rejected the request because my E-Mail adress was not listed in the trusted_puppetmaster_hosts. However,
I still think this is a security bug.

The issue is caused by the defaults of the puppetlabs apache module, which turns into a problem if SSL
Client authentication is used.
There were also upstream Pull requests against the puppetlabs module, which to allow unset this Parameter, but unfortunately the default was not changed:

https://github.com/puppetlabs/puppetlabs-apache/pull/787
https://github.com/puppetlabs/puppetlabs-apache/pull/913

The foreman puppet modules (puppet-foreman, puppet-puppet) should explicitly unset ssl_certs_dir when configuring apache vhosts.

Associated revisions

Revision 08911c3a - 01/14/2016 09:58 AM - Markus Frosch

fixes #11652: set ssl_certs_dir to '' by default

This will avoid setting SSLCACertificatePath by default. And that way only request and authenticate certificates by the configured CA and not any other present in the certs directory.

History

#1 - 09/02/2015 05:10 AM - Dominic Cleal

- Project changed from Foreman to Installer

- Category changed from Authentication to Foreman modules

#2 - 01/18/2016 11:02 AM - Markus Frosch

- Status changed from New to Closed

- % Done changed from 0 to 100

Applied in changeset puppet-foreman|08911c3a6c776462fcc1aa99103fe588b8feb365.

#3 - 01/19/2016 08:19 AM - Dominic Cleal

- translation missing: en.field_release set to 71