Foreman - Bug #19416

Unable to verify LDAPS certificate

04/27/2017 12:52 PM - Sindre Grindvoll

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

Description

When trying to connect to a Windows Active Directory with LDAP over SSL (LDAPS), the connection fails due to not being able to verify the certificate. The root certificate have been added as a trusted CA on the Foreman server.

Guides and tips from the following issues and documentation have been tried:
- #10139 - http://projects.theforeman.org/issues/2435
- #9858 - http://projects.theforeman.org/issues/9858
- https://theforeman.org/manuals/1.14/index.html#4.1.1LDAPAuthentication

Nothing changes the outcome when trying to connect to the AD server using LDAPS, however no problem with LDAP.
Communication with LDAPS is working when disabling the certificate verification in the Foreman configuration:

```
/usr/share/foreman/app/models/auth_sources/auth_source_ldap.rb
```

Changing VERIFY_PEER to VERIFY_NONE allows communication with LDAPS.
93   { :method => :simple_tls, :tls_options => { :verify_mode => OpenSSL::SSL::VERIFY_PEER / NONE } }

System information:
- Ubuntu 16.04 Xenial
- Puppet version 4.9.2
- Foreman version 1.12.4
- Foreman installation guide used: https://marcusit.com/setting-up-puppet-and-foreman-on-ubuntu-16-04-part-i/

History

#1 - 04/28/2017 03:39 AM - Marek Hulán

could you double check that you installed the certificate of a CA that you (should) see when running

```
openssl s_client -showcerts -connect ad_host:port
```

we're using standard openssl verification so it's very likely something with the configuration

#2 - 04/28/2017 03:40 AM - Marek Hulán

- *Project changed from Website to Foreman*

- *Category set to Authentication*

#3 - 05/01/2017 11:28 AM - Sindre Grindvoll

Thanks for the quick reply!

The output verifies that the correct CA is installed.

#4 - 05/17/2017 04:18 PM - Karli Sjöberg

Sindre Grindvoll wrote:

> Thanks for the quick reply!

> The output verifies that the correct CA is installed.

I have just solved this problem myself and thought of opening a new issue but found this open and didn´t want to spam issues so I'm adding to this instead, even though it might not be related to your situation, apologies in advance:)

I had also added my CA to the system´s root bundle and restarted apache but couldn´t get it going either, until I edited the previously mentioned file "/usr/local/share/foreman/app/models/auth_sources/auth_source_ldap.rb" like this: ########
--- /usr/local/share/foreman/app/models/auth_sources/auth_source_ldap.rb 2017-05-17 21:30:45.804696000 0200
++ /usr/local/share/foreman/app/models/auth_sources/auth_source_ldap.rb 2017-05-17 21:31:27.883089000 +0200
@ -95,7 +95,7 @ ########

```
def encryption_config
     return nil unless tls
-    { :method => :simple_tls, :tls_options => { :verify_mode => OpenSSL::SSL::VERIFY_PEER } }
+    { :method => :simple_tls, :tls_options => { :ca_file => "/usr/local/etc/ssl/cert.pem", :verify_mode => OpenSSL::SSL::VERIFY_PEER } }
   end
```

```
def ldap_con(login = nil, password = nil)
```

After another restart of apache, it worked like a charm!

@Marek Hulán
My Foreman server is running on FreeBSD, which is why the CA bundle is called like that. What´s it called in other distros like CentOS, Debian and so forth? Would it be possible to ifdef based on operatingsystem what "tls_options" becomes, we could just add exceptions to the default based on that? Would that be an acceptable solution? I´m just thinking out loud for the sake of better platform support.

Best Regards
Karli Sjöberg

#5 - 05/17/2017 04:39 PM - Karli Sjöberg

- File auth_source_ldap.rb.patch added

Hi again!

I got inspired and made a patch that adjusts "tls_options" if running on FreeBSD, plus that I forgot to format the patch in my previous post as "code" so it looked weird, a patch file is better. Tested with Foreman 1.14.1.

/K

#6 - 05/18/2017 02:27 AM - Marek Hulán

Thanks Karli, could you please open a PR with the patch at https://github.com/theforeman/foreman? I think it would get accepted. If you're unsure about how to do it, please see https://theforeman.org/contribute.html#SubmitPatches

#7 - 05/18/2017 01:44 PM - Karli Sjöberg

Marek Hulán wrote:

> Thanks Karli, could you please open a PR with the patch at https://github.com/theforeman/foreman? I think it would get accepted. If you're unsure about how to do it, please see https://theforeman.org/contribute.html#SubmitPatches

Absolutely, here you have it:
https://github.com/theforeman/foreman/pull/4539

Thank you for the links, I don´t do this often enough to remember it:)

/K

#8 - 05/25/2017 03:53 PM - Karli Sjöberg

Hello again!

After discussing it with a couple of developers, I decided to scrap the PR, it isn´t needed actually. Apparently, in FreeBSD, there are several CA bundles and I added my CA to one that ruby doesn´t look in:)

@Sindre Grindvoll
I wrote this script that prints ruby´s CA settings:

/usr/share/foreman/test_ssl.rb:

require "openssl"

```
puts "SSL_CERT_FILE: %s" % OpenSSL::X509::DEFAULT_CERT_FILE
```

1. sudo -u foreman ruby /usr/share/foreman/test_ssl.rb

Then you will know what file you need to add your CA to.

Best Regards
Karli Sjöberg

#9 - 05/25/2017 03:56 PM - Sindre Grindvoll

Amazing response to this issue! Thank you so much guys.

I havn't had the oportunity to continue the troubleshooting for a little while, but will try out the fix next week!

#10 - 05/26/2017 03:04 AM - Dominic Cleal

- Status changed from New to Feedback

#11 - 06/05/2017 08:06 AM - Sindre Grindvoll

I tried out your script which returns the default keystore in use by Ruby. The funny thing, is that the keystore the script returns doesn't exist on the VM I'm running this on. This means that ruby can't find the CA when it tries to verify the LDAPS connection. Unfortunately I don't have time to do further troubleshooting at the moment, but I do think this is the answer to my problems.

Files

auth_source_ldap.rb.patch	983 Bytes	05/17/2017	Karli Sjöberg