Installer - Bug #29279

Drop use of SSLCertificateChainFile and combine CA certs

03/06/2020 02:05 PM - Eric Helms

Status:	New		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

See documentation here https://httpd.apache.org/docs/current/mod/mod_ssl.html#sslcertificatechainfile

History

#1 - 03/06/2020 02:22 PM - Ewoud Kohl van Wijngaarden

That's not how we use it. We use SSLCertificateChainFile as the CA that allows client authentication and SSLCACertificatePath to serve the CA chain to the client. This is because we have 2 different CA chains that are being served.

#2 - 03/13/2024 11:25 AM - Rune Philosof

Ewoud Kohl van Wijngaarden wrote in #note-1:

> That's not how we use it. We use SSLCertificateChainFile as the CA that allows client authentication and SSLCACertificatePath to serve the CA chain to the client. This is because we have 2 different CA chains that are being served.

I think you mixed up some definitions

From apache documentation:

- SSLCACertificatePath will be used for both client authentication and server certificate chain.
- SSLCertificateFile will be used for server certificate and chain
- SSLCertificateChainFile will be used for server certificate and chain
- SSLCACertificateFile containing a list of ca pem certs, will be used for client authentication

Foreman is not using `SSLCACertificatePath`, which would be `ssl_certs_dir` here https://github.com/theforeman/puppet-foreman/blob/ea57c5ceb0ba99a241e5c93b708dc0f010e38c47/manifests/config/apache.pp#L318. And it should not.

It seems the `server_ssl_ca` is used as SSLCACertificateFile, which is for client authentication, see
https://github.com/theforeman/puppet-foreman/blob/ea57c5ceb0ba99a241e5c93b708dc0f010e38c47/manifests/config.pp#L159
I suggest removing `server_ssl_ca` and using `client_ssl_ca` instead.

1. `server_ssl_chain` should default to empty.
2. The generated `server_ssl_cert` file should contain the ca chain.

I am unsure about migration.
Changing the default to empty, existing installations using the foreman installer generated certificates would start to fail, since their `server_ssl_cert` file does not contain the CA.
If it can be detected whether an installation is using the default generated certs (a) or self-supplied certs (b), then maybe (a) should have their existing `server_ssl_chain` file appended to their `server_ssl_cert` file.