Installer - Bug #37029

YAML scenario - server_ssl_chain is ignored

01/04/2024 02:19 PM - Francesco Di Nucci

Status:	New		
Priority:	Normal		
Assignee:			
Category:	foreman-installer script		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	3.8.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Hello,
I'm installing Foreman 3.8.0 on AlmaLinux 8.9, using a custom scenario YAML. I'm setting up SSL/TLS, so amongst other options there are the following:

```
foreman:
  apache: true
  ssl: true
  server_port: 80
  server_ssl_port: 443
  server_ssl_ca: /etc/pki/tls/certs/foreman-ca.pem
  server_ssl_chain: /etc/pki/tls/certs/foreman-ca.pem
  server_ssl_cert: /etc/pki/tls/certs/foreman-cert.pem
  server_ssl_key: /etc/pki/tls/private/foreman-private.key
  server_ssl_crl: /etc/pki/tls/certs/foreman-crl.pem
  server_ssl_verify_client: optional
  client_ssl_ca: /etc/pki/tls/certs/foreman-ca.pem
  client_ssl_cert: /etc/pki/tls/certs/foreman-cert.pem
  client_ssl_key: /etc/pki/tls/private/foreman-private.key
  websockets_encrypt: true
  websockets_ssl_key: /etc/pki/tls/private/foreman-private.key
  websockets_ssl_cert: /etc/pki/tls/certs/foreman-cert.pem
```

The issue is that although server_ssl_chain is specified, it is not set in /etc/httpd/conf.d/05-foreman-ssl.conf, where it defaults to SSLCertificateChainFile "/etc/puppetlabs/puppet/ssl/certs/ca.pem"

Also, I'm not sure SSLCertificateChainFile should be set at all, because *SSLCertificateChainFile became obsolete with version 2.4.8, when SSLCertificateFile was extended to also load intermediate CA certificates from the server certificate file.* [See https://httpd.apache.org/docs/current/mod/mod_ssl.html#sslcertificatechainfile]

History

#1 - 01/04/2024 02:21 PM - Francesco Di Nucci

Currently using:

- AlmaLinux 8.9 (Midnight Oncilla)
- foreman-installer-3.8.0-2.el8.noarch

#2 - 03/11/2024 02:55 PM - Ewoud Kohl van Wijngaarden

> I'm installing Foreman 3.8.0 on AlmaLinux 8.9, using a custom scenario YAML. I'm setting up SSL/TLS, so amongst other options there are the following:

Can you share a bit more about how you you did this?

> The issue is that although server_ssl_chain is specified, it is not set in /etc/httpd/conf.d/05-foreman-ssl.conf, where it defaults to SSLCertificateChainFile "/etc/puppetlabs/puppet/ssl/certs/ca.pem"

This is odd, because I don't see why it wouldn't work.

> Also, I'm not sure SSLCertificateChainFile should be set at all, because SSLCertificateChainFile became obsolete with version 2.4.8, when SSLCertificateFile was extended to also load intermediate CA certificates from the server certificate file. [See https://httpd.apache.org/docs/current/mod/mod_ssl.html#sslcertificatechainfile]

From the Apache docs you linked:

> This should be used alternatively and/or additionally to SSLCACertificatePath for explicitly constructing the server certificate chain which is sent to the browser in addition to the server certificate. It is especially useful to avoid conflicts with CA certificates when using client authentication. Because although placing a CA certificate of the server certificate chain into SSLCACertificatePath has the same effect for the certificate chain construction, it has the side-effect that client certificates issued by this same CA certificate are also accepted on client authentication.

This is a use case we rely on: we have a CA that signed the server certificate, but that can be a different CA than the CA that accepts client certificates. That's why I've never been able to determine a path forward (though I also haven't spent a lot of time on it).

#3 - 03/13/2024 10:55 AM - Rune Philosof

Ewoud Kohl van Wijngaarden wrote in #note-2:

> I'm installing Foreman 3.8.0 on AlmaLinux 8.9, using a custom scenario YAML. I'm setting up SSL/TLS, so amongst other options there are the following:

Can you share a bit more about how you you did this?

> The issue is that although server_ssl_chain is specified, it is not set in /etc/httpd/conf.d/05-foreman-ssl.conf, where it defaults to SSLCertificateChainFile "/etc/puppetlabs/puppet/ssl/certs/ca.pem"

This is odd, because I don't see why it wouldn't work.

Could it be because `$ssl_ca_file` is preferred over `$foreman::server_ssl_chain` here
https://github.com/theforeman/puppet-foreman/blob/ea57c5ceb0ba99a241e5c93b708dc0f010e38c47/manifests/cli.pp#L44

I suggest making an e2e spec that checks the foreman-ssl content given that yaml input.

> Also, I'm not sure SSLCertificateChainFile should be set at all, because SSLCertificateChainFile became obsolete with version 2.4.8, when SSLCertificateFile was extended to also load intermediate CA certificates from the server certificate file. [See https://httpd.apache.org/docs/current/mod/mod_ssl.html#sslcertificatechainfile]

From the Apache docs you linked:

> This should be used alternatively and/or additionally to SSLCACertificatePath for explicitly constructing the server certificate chain which is sent to the browser in addition to the server certificate. It is especially useful to avoid conflicts with CA certificates when using client authentication. Because although placing a CA certificate of the server certificate chain into SSLCACertificatePath has the same effect for the certificate chain construction, it has the side-effect that client certificates issued by this same CA certificate are also accepted on client authentication.

This is a use case we rely on: we have a CA that signed the server certificate, but that can be a different CA than the CA that accepts client certificates. That's why I've never been able to determine a path forward (though I also haven't spent a lot of time on it).

I disagree, but I will comment on that in https://projects.theforeman.org/issues/29279

#4 - 03/25/2024 09:40 AM - Francesco Di Nucci

Meanwhile I switched to Foreman 3.9, the installer does not have this issue (or I wasn't able to reproduce it), feel free to close/reject the issue