Foreman - Feature #25469

Better handling of smart proxy certificate and secrets generation and distribution

11/14/2018 11:34 PM - Alan Evans

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

Description

Most security best practices **recommend against** things like:

1. Keeping unnecessary copies of private keys
2. Providing passwords (secrets) on the commandline

The current process of running `foreman-proxy-certs-generate`, copying *-certs.tar to a smart proxy, then running `foreman-installer --scenario foreman-proxy-content --foreman-proxy-content-certs-tar` has users doing both of these things.

Yes, it is ultimately the responsibility of the System Administrator using Foreman to understand these best practices and to take mitigating actions, like securely erasing unnecessary intermediate files and removing entries from shell histories, but that doesn't mean Foreman shouldn't attempt to do things better.

Proposal

1. Add APIs for certificate request and signing
2. Add APIs for smart proxy retrieval of secrets using certificate auth (actually could foreman just use certificate auth instead of secrets?)

In this ticket I focus on smart proxies, but a generic certificate request/signing API may have other uses. I would suggest integrating with the puppet CA but I think that might cause other problems.