

Foreman - Tracker #34842

Support EC (and other non-RSA) keys for authentication

05/02/2022 07:30 AM - Evgeni Golov

| | |
|-------------------------|---------------------------------|
| Status: New | % Done: 36% |
| Priority: Normal | |
| Assignee: | |
| Category: | |
| Target version: | |
| Difficulty: | Fixed in Releases: |
| Triaged: No | Found in Releases: 3.3.0 |
| Bugzilla link: | Red Hat JIRA: |

Description

It's the year 2022, we should support non-RSA (especially elliptic curve) keys for authentication in the project.

The list of associated tasks is generated using as simple git grep 'OpenSSL.*RSA', which might not be complete.

In most cases, the change should be as trivial as:

```
-      OpenSSL::PKey::RSA.new(File.read(path))  
+      OpenSSL::PKey.read(File.read(path))
```

as that allows OpenSSL to figure out what kind of key it gets, instead of forcing RSA.

Subtasks:

| | |
|--|-------------------|
| Feature # 34843: Support EC (and other non-RSA) keys in Foreman core | Closed |
| Feature # 34844: Support EC (and other non-RSA) keys in foreman proxy | Closed |
| Feature # 34845: Support EC (and other non-RSA) keys in discovery | Ready For Testing |
| Feature # 34846: Support EC (and other non-RSA) keys in scap client | Ready For Testing |
| Feature # 34847: Support EC (and other non-RSA) keys in webhooks | Closed |
| Feature # 34848: Support EC (and other non-RSA) keys in proxy chef | New |
| Feature # 34849: Support EC (and other non-RSA) keys in proxy monitoring icinga2 | New |
| Feature # 34850: Support EC (and other non-RSA) keys in proxy salt | New |
| Feature # 34851: Support EC (and other non-RSA) keys in proxy vault | New |
| Feature # 34852: Support EC (and other non-RSA) keys in Katello | New |
| Feature # 34853: Support EC (and other non-RSA) keys in hammer | Closed |

History

#1 - 05/02/2022 07:43 AM - Evgeni Golov

- Description updated