DevOps Secrets Safe 20.3 Release Notes

July 14, 2020

Requirements:

- DevOps Secrets Safe deployment is currently supported using Helm 3.
- DevOps Secrets Safe is currently supported on Kubernetes version 1.13, 1.14, 1.15, 1.16, 1.17.
- DevOps Secrets Safe CLI (ssrun) is supported on any standard Unix / Linux environment that has Python 3.5 or higher and pip3 installed.
- The MD5 signature is: dcb51988197daf212a298816f1c9f9b5.
- The SHA-1 signature is: 36a38221ff6bfcf1d4770a81e2a5e1c26409dfb9.

New Features and Enhancements:

- Kubernetes Integration:
  - The new Kuberenetes Identity Provider allows usage of Kubernetes service account tokens as credentials for external principals in DSS.
  - Kubernetes applications can retrieve secrets from DSS using the secret-retriever init container.
- Secrets Safe has now been certified as compatible with AWS EKS Managed Kubernetes Service.
- A new Puppet module is available which allows for storage and retrieval of secrets in DSS.
- A new Ansible module is available which provides the capability to store secrets in DSS.
- The Duo authentication provider may now be used to provide a second factor for authentication.
- Upgrade in Place:
  - Secrets Safe versions may now be upgraded without first uninstalling, to minimize downtime.
  - Secrets Safe installer and uninstaller no longer support Helm 2.
- Refresh tokens are now supported to allow CLI or API clients to acquire new access tokens without full re-authentication.
- It is now possible to configure access token duration, refresh token duration, and maximum request sizes at the global level.

Notes:

- API request throughput under load is improved.